Group HW
Class 40
Piece 181

F

15 Q. Part II.
PERS 2-5

GC
1178

Authority to close: Victor [illegible]
Date: 26th Jan., 1949

PUBLIC RECORD OFFICE

Group/Class HW 40

Piece 181

Papers relating to the Post-war period retained under S3(4) of the PRA (1958)

(date) 11/2/2004

(Signed)

15(a)

20 Grosvenor Square.

(23)

A8/mdj

17 September 1947.

SECRET

MEMORANDUM FOR: Director, L.S.I.C.

(Attention: TICOM).

Subject: Interrogation of Selchow.

1. The attached TICOM report is transmitted herewith for your information. If you consider further interrogation of SELCHOW, I will so inform the authorities at ASA Europe.

William G Bartlett

WILLIAM G. BARTLETT,
Lt. Col., GSC., U.S.Army,
Senior U.S. Liaison Officer.

SECRET

HW 40/181

15(a)

SECRET

APO 757

ASA-13/MCL/ab

3 September 1947

SUBJECT: Interrogation of Selchow

TO: IDWD Detachment
c/o Military Attache
London, England
Naval Fleet Post Office No. 100
(to be passed to TICOM)

1. Pursuant to request of Army Security Agency, Washington for information concerning Selchow of the German Ministry of Foreign Affairs, the inclosed report is forwarded as a preliminary interrogation report of Selchow conducted by a representative of Army Security Agency, Europe at Frankfurt am Main, 2 September 1947.

2. It is requested that this Headquarters be advised whether further interrogation of Selchow is desired by TICOM, and if so, that specific questions be forwarded to this Headquarters for use in the interrogation.

3. A copy of the inclosed report has been forwarded to Army Security Agency, Washington and that Agency has also been requested to advise whether further interrogation is desirable.

Incl
Report of Interrogation

ROBERT T. WALKER
Lt. Colonel, Signal Corps
Chief

SECRET

15 (i)

TOP SECRET

TICOM/I-208

24

INTERROGATION REPORT ON KURT SELCHOW, FORMER HEAD OF THE PERS ZS DEPARTMENT OF THE GERMAN MINISTRY OF FOREIGN AFFAIRS.

Attached is a report on the interrogation of Gesandter Ministerdirigent Kurt SELCHOW, former head of "Pers ZS", the crypto-bureau of the German Ministry of Foreign Affairs, carried out at Frankfurt-am-Main on 2nd September, 1947, by Captain Mary C. LANE of A.S.A. Europe.

2. The report is of general historical interest, and SELCHOW claims to have no technical knowledge. For detailed interrogation report on the work of his department, including the personnel mentioned by him on page 10, see Ticom/I-22.

TICOM
27th October, 1947.

No. of Sheets: 3

Copy No: 11.

Distribution :-

L.S.I.C.

1. T.
2. S.
3. H.
4. Brigadier Tiltman.
5. L.
6. Z.
7. H.71
8. R.1 for Dr. Morgan.
9-10. Z.86.
11. L.91.
12-15. Ticom Files.

U.S.L.O.

16. U.S.L.O.
17-20. Op-20-2.)
21-24. A.S.A. Washington.) via U.S.L.O.
25. Chief, A.S.A. Europe.)

TOP SECRET

INTERROGATION REPORT ON KURT SELCHOW, FORMER HEAD OF THE PERS ZS DEPARTMENT OF THE GERMAN MINISTRY OF FOREIGN AFFAIRS.

Personal Data:

a.	Surname:	SELCHOW.
b.	Christian Names:	Kurt Richard.
c.	Aliases:	None.
d.	Date and Place of Birth:	28 May 1886. Oppeln, Upper Silesia, Germany.
e.	Nationality claimed:	German.
f.	Occupation:	Former head, with rank of Gesandter Ministerdirigent, of Cryptobureau, German Ministry of Foreign Affairs.
g.	Religion:	Evangelical.
h.	Description:	
	Height:	Approximately 6'2".
	Weight:	Approximately 160 pounds.
	Build:	Thin, tall.
	Face:	Square, grey-blue eyes, glasses.
	Hair:	Slightly grey and thinning.
i.	Last Permanent Address:	Wedel bei Hamburg, Schulauerstrasse 9.
j.	Father:	Hugo SELCHOW, Postdirektor at Oppeln (deceased).
k.	Mother:	--------
l.	Brothers:	--------
m.	Sisters:	--------
n.	Wife:	Erna SELCHOW (geboren Schultz).
o.	Children:	One daughter, Gitta.
p.	Identity documents:	Certificate of identity from Office of Chief of Counsel, Nuernberg. Identification card.

Autobiographical Notes: SELCHOW, Kurt Richard was born 28 May, 1886, in Oppeln, Upper Silesia, Germany, the son of the Postdirektor of Oppeln, Hugo SELCHOW. He was educated in the schools of Oppeln until 1906 when he became a soldier. Assigned at first to the Infantry, he was transferred in 1912 to the Signal Corps (Nachrichten Telegrafen Bataillon) in Frankfurt-an-Oder. He served with the German Army of World War I as a signal officer with the troops. SELCHOW stated that even in the midst of World War I he had pointed out to the Chief Signal Officer that much of the work being done in the German Army Signal Corps belonged properly to the German Ministry of Foreign Affairs because of its diplomatic nature. The Chief

Please turn over

Signal Officer did not agree with this statement and during the war much of the work done by the Army was diplomatic. Directly after World War I, however, SELCHOW entered the German Ministry of Foreign Affairs where he organised the crypto-bureau. He brought with him into the crypto-bureau several soldiers whom he had known during the war, viz: SCHAUFFLER, PASCHKE, ZASTROW, BRANDES, HOFFMANN and KUNZE. He remained head of the crypto-bureau until the defeat of Germany in May, 1945. After the defeat of Germany, SELCHOW remained for two years in the French Zone of Germany at Weiler/Vorarlberg, Swabia.

In mid-April, 1947, SELCHOW moved to Wedel bei Hamburg, British Zone of Germany, where he now lives with his wife and daughter in the house of a relative. He is employed in a merchant firm of a relative in Wedel, and his daughter is employed in a factory owned by a relative in Wedel, His wife is ill. SELCHOW expressed the desire to move with his wife and daughter to the American Zone of Germany, preferably to Marburg where he stated, SCHAUFFLER, PASCHKE and KUNZE now live. He has, however, no means of obtaining the necessary permission of Military Government to come into the American Zone and procure a residence.

Contact with Foreign Governments since End of War: SELCHOW stated that although he lived for two years in the French Zone of Germany after the end of the war he had not spoken with any French authorities concerning his previous occupation. He stated that when the French had discovered on his identification papers that he had been the head of the Crypto-bureau of the German Ministry of Foreign Affairs they stated that all the crypto-systems had changed and hence they were not interested in questioning him. Once, however, he had learned that for some time it had been thought by the French that his name was a cover-name for a system (the Selchowsysteme). SELCHOW stated that he had never been questioned by the British during his residence in Wedel concerning his previous occupation.

Contact with Former Colleagues: SELCHOW stated that he was in frequent communication by letter with other former members of the German Ministry of Foreign Affairs, particularly those who had been his colleagues during the entire period of his service with the Ministry of Foreign Affairs. As stated above, PASCHKE, SCHAUFFLER and KUNZE were said to be living in Marburg; HOFFMANN, Ernst, Former head of the Funkbuero and Fernschreibstelle of the crypto-bureau was now living in Minden/Westfalien. Dr. HAUTHAL was living at Alten Hohenau/Post Griesstaett/Inn. He stated that Dr. ROY, who had been head of the Verwaltungsbuero of the crypto-bureau had been for some time after the war in a prison camp at Halle/Saale, but was now a prisoner in Russia and had not been heard from for some time.

Notes on History of Crypto-bureau of Ministry of Foreign Affairs: SELCHOW stated that he was familiar with the history of the crypto-bureau of the Ministry of Foreign Affairs from 1919 to 1945. Such a bureau had existed within the Ministry of Foreign Affairs during World War I, but chiefly as an enciphering and encoding group. In 1919, when he became leader of this group, he introduced the system of dividing work upon foreign codes and ciphers into sections for the various countries and selected as leaders of these sections those men such as PASCHKE, KUNZE and SCHAUFFLER who had been known to him during the War. The crypto-bureau had been before 1919 and continued to be throughout World War II subordinated to the Personalabteilung of the Ministry of Foreign Affairs.

The outline of the chain of command within the Ministry and the organisation of the crypto-bureau as he described it is as follows :-

Please turn over

Auswaertiges Amt

Personalabteilung - Herr SCHROEDER

Personalabteilung Z - Ministerialdirigent Gesandter SELCHOW

I Chiffrierbuero Verwaltungsbuero	II Anfertigung der Chiffrier- verfahren Verzifferung und Entzifferung	III Nachrichten- uebermittlung Funkbuero Fernschreibstelle Presse and Radio Aufnahme	IV Entzifferung fremder Verfahrungen Sprachgruppe PASCHKE SCHAUFFLER Technische Gruppe KUNZE
ROY	HAUTHAL	HOFFMANN	

SELCHOW stated that during the latter years of World War II the crypto-bureau of the Ministry of Foreign Affairs had expanded until it comprised between 400 and 500 persons, including both men and women. However, it had up to that time remained relatively small and at the beginning, the group had consisted of only fourteen or fifteen persons.

At the end of the war the crypto-bureau had been forced by bombing to leave Berlin-Dahlem and to move successively southward. This accounted for the presence of SELCHOW near Weiler at the end of the war and for his continued residence in the French Occupied Zone of Germany.

Relation of SELCHOW to OKW/Chi and to the Forschungsamt: SELCHOW was particularly anxious to clear his record of any voluntary relation with the National Socialist Party. He stated that from the very beginning of his diplomatic career he had been interested in a closer co-operation of the various countries of Europe with one another, on something of the same plan now advocated by CHURCHILL. He had not been a militarist, nor had he interested himself in military systems, making it a strict policy within the Ministry of Foreign Affairs that only systems of a diplomatic nature should be dealt with. Until 1933 the crypto-bureau of the Ministry of Foreign Affairs had had the entire field of diplomatic ciphers to itself. The cryptographic systems of the Armed Forces of other countries were handled by the Wehrmacht. With the advent of HITLER, however, the Luftfahrtministerium under GOERING encroached upon the field of the cryptobureau of the Ministry of Foreign Affairs. SELCHOW stated that he himself at this time wished to resign since he had no sympathy whatsoever with the National Socialist movement. He was persuaded to remain, however, by von BULOW who was until 1938 Secretary of the Ministry of Foreign Affairs. Von BULOW, who was also a firm opponent of National Socialism, was extremely anxious that the crypto-bureau of the Ministry of Foreign Affairs remain untarnished by National Socialism and that it be staffed by opponents to the new movement. SELCHOW therefore remained with the crypto-bureau but outside the National Socialist Party until von BULOW's death in 1938. When RIBBENTROP became head of the Ministry of Foreign Affairs a great deal of power was taken from SELCHOW, since von RIBBENTROP did not trust him. His supervisory capacity was restricted to those sections which dealt with the passing of messages to and from missions and to the technicalities of the deciphering of the systems of foreign countries. He was forced to join the Party in 1941 but took no active part in its policy. During the war years he had no exact knowledge of the messages passed and took no part in any matters pertaining to diplomacy.

SELCHOW stated that when he and his colleagues in the crypto-bureau were ordered to collaborate with the personnel of the Forschungsamt, they often gave false information concerning systems or solution of systems in order to

Please turn over

TOP SECRET

hinder as much as possible the work of that organisation. On the other hand, as the war progressed collaboration with OKW/Chi grew better, particularly on new problems on which all worked in common.

Impression of Interrogator: It was the impression of the interrogator that SELCHOW was extremely co-operative. He talked swiftly and with an eager enthusiasm concerning his past activity. He denied all technical knowledge but stated that KUNZE, SCHAUFFLER and PASCHKE could give technical details. He was familiar with the fact that these men had been interrogated by the British and the Americans and stated that they had already given full reports to the authorities in those countries.

There is no doubt that SELCHOW possesses much valuable historical knowledge concerning the development, organisation and personnel of the crypto-bureau of the Ministry of Foreign Affairs. He is evidently in close contact with former members of the crypto-bureau and offered to come to Marburg where PASCHKE, SCHAUFFLER and KUNZE now are and collaborate with them on a complete history of the development, organisation and technical successes of the bureau. He was quite certain that he could also bring HOFFMANN and HAUTHAL into this work, should the United States government wish it. The interrogator stated that this proposal would be referred to the United States government and that he would be informed at Wedel, should further interrogation be required. SELCHOW stated that should he be forced by circumstances to move from his present residence at Schulauerstrasse 9, PASCHKE of Marburg would know where he could be reached.

at end 1943

uswertiges Amt

Pers. Z. S.

Staats Sekretaar (Weyacker '37-44
Steegracht 44-45)

Schroder

Director: Minister 1st. class SELCHOW

Main Dept. - Berlin - Dahlem
ORR. SCHAUFFLER
PASCHKE

SCHAUFFLER
1. Japan
2. Systems & research
3. Applying, experience on foreign cyphers to home systems.

PASCHKE:
1. Admin.
2. Working on & editing of diplomatic tle grams of foreign countries:-

a) Japan, China	ORR.	SCHAUFFLER
b) Turkey	ORR	SCHERSCHMIDT
c) Iran, Afghanistan	RR.	Dr. BENZING
d) Italy, Greece.	ORR.	PASCHKE
e) France, Belgium, Swiss.	RR.	BRANDES
f) Rumania	RR	Dr. KASPER.
g) Yugoslavia		Dr. KRUMMEL
h) U. S. A.		ZASTROW
i) England, Ireland, Spain, Portugal, Latin America.		Frl. HAGEN – Herr Hoffman from 1922 - 1939

3. Information & intelligence card index. — Dr. HORN.

Alternative Station HIRSCHBERG (Rusenjebige)
RR Dr. KARSTIEN

a. Crypto commitments
  1. Book building
  2. Handling, translation & editing telegrams not of an urgent nature.
  3. Current breaking of difficult recyphers.

b. Territories:
  a. Bulgaria, Croatia, Poland (RR. Dr. KARSTIEN)
  b. Japan, China (Dr. OLBRICHT)
  c. Frane, Belgium, Swiss (Frl. SCHRADER)

Staats Sekretär (Von Steengracht)

Ministerial Direktor Schröder — Gesandter Bergmann (held by Russians)

[illegible] ([illegible] 1945)

|

[illegible]

|

II

[illegible] X

I

[illegible] X

III

[illegible] X

[illegible]

[illegible]

[illegible] Sections by countries:-

1. France, Belgium, Switzerland, Holland. [illegible] X
   Deputy: [illegible] X
2. Gr. Britain, Ireland, Spain, Portugal, Central & South America [illegible]
   Head of Sec. [illegible] Frl. [illegible] X
   Deputy: [illegible]
3. Italy, Vatican, Greek, USSR
   Head of Sec. ORR PASCHKE X — Frau ~~Dr~~ Paschke
   Deputy: WHA Dr. DEUBNER X
4. [illegible]
   Head of Sec. RR. Dr. KASPER.
   Deputy WHA MENNING
5. [illegible] ([illegible])
   Esthonia, Lithuania
   Head of Sec. [illegible] Dr. [illegible] X
   Deputy [illegible] X
6. [illegible] Scandinavia
   Head of Sec. WHA Dr. MUELLER (HANS KURT) X
   Deputy [illegible] X
7. Turkey
   Head: [illegible] X ?
8. [illegible] Arab States.
   Head [illegible] Dr. [illegible] X
   Deputy [illegible]
9. Japan, China [illegible]
   Head ORR SCHAUFFLER
   Deputy [illegible] X

B. Office, information & files. Head Prof. Dr. [illegible]

Alt [illegible] ([illegible])

[illegible]

[illegible]

X [illegible]

TOP SECRET

15(2)

4 NOV 1946

(2)

24 October 1946

MEMORANDUM FOR MAJOR E. DALE MARSTON

From Chief ASA-14: As an item of historical interest to TICOM we would like to suggest that the signature SCHAPPER, FIRST LIEUTENANT AND COMMANDER appearing on pp. 20 and 34, inter alia, of D-82, "Camouflaged Secret Writing," a translation of Ticom Document 3294 (Pers ZS papers and correspondence of 1917) is that of Gottfried Schapper, the last head of the Forschungsamt. Schapper gave an autobiography (cf Final Report of TICOM Team 1, Appendix 2) which stated that in 1916-17 he was Director of the Cryptographic Bureau of the High Command of the Army. This identification is considered to be of interest since it affords one of the few checks on the credibility of Schapper. It also suggests the possibility of further questioning of Schapper (believed to be still a prisoner as a former member of the Nazi Party and SS) if warranted as of historical interest for World War I.

Fred Griffin
FRED GRIFFIN

L 91
Your Info
E D Marston

TOP SECRET

Copy to L. 12/10

TICOM/D-31 [redacted] SECRET

20

CORRESPONDENCE REGARDING THE [illegible] OF SECURITY OF CRYPTOGRAPHIC SYSTEMS OF THE GERMAN FOREIGN OFFICE.

The attached translation by A.S.A. Washington is of an item from TICOM document T.5297, entitled CRYPTOGRAPHIC ITEMS FROM FILES OF GERMAN FOREIGN OFFICE.

2. The correspondence is dated 1917 and relates in the main to systems supplied to German Naval Attachés by the German Foreign Office and found insecure on examination by the cryptanalysts of the German Naval Staff.

3. Historically this is of interest as an early case of detailed cryptanalytic examination of cryptographic material from a defence angle.

TICOM
7th October, 1946.

No. of pages: 11
Copy No: 8

Distribution:-

British

[illegible]

[illegible]

[illegible]

[illegible]

[illegible] the Foreign Office [illegible] with the embassies in [illegible] with the mission in Persia. The embassy in [illegible]

[illegible]
enemies since they had to be enciphered with a cipher which
[illegible]

[illegible]

T O P   S E C R E T

[illegible] ight be in a position [illegible]

[illegible]

[illegible]

[illegible]

[illegible] of the Foreign Office
[illegible] Headquarters [illegible]
[illegible]

[illegible] Secretary of State [illegible]

[illegible]

TOP SECRET

Chief of the Admiralty Sta[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

Chief of the Admiralty Staff
[illegible] of the Navy
[illegible]

Berlin, [illegible] 1917.

Very Secret.

To [illegible] Chief of the General Staff of the Field Army, [illegible]

Enclosed I send Your Excellency for your information a copy of a letter to the [illegible] of the Foreign Office.

[illegible] to use caution in transmitting secret material through the [illegible] of the Foreign Office.

(Signed) [illegible]

Chief of the General Staff of the Field Army
No. 5119 Secret

Great Headquarters
7 [illegible] 1917.

Only by Officer

[illegible]

[illegible]

[illegible]

[illegible]

TOP SECRET

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

TOP SECRET

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

TOP SECRET

Chief of Communications Service
Section IV c Nr. 742[illegible]
[illegible] 18 VIII out 17 VIII 17

It was assumed [illegible] with the inscription "Minister of Foreign Affairs Madrid" and "Minister of Foreign Affairs Berlin" was conducted by the Foreign Office, or [illegible] there. From the above communication from the Foreign Office, as well as from solution of another system [illegible] this traffic which has been [illegible] the Section [illegible], it appears that this is not the case. The [illegible] as yet unsolved systems from this traffic, among which [illegible] of the Foreign Office must be found, are [illegible] worked on [illegible].

[illegible]

V. d. Ch. d. N.
i. Ch. d. N.
(Signed) von [illegible]

Berlin, [illegible] August 1917

Foreign Office
[illegible]
[illegible]
Reply to letter of [illegible] of this year.
[illegible] Subject
[illegible]
Very Secret

Representative of the Foreign Office in Grand Headquarters
Nr. 65[illegible]
[illegible] 19 VIII 17
[illegible] von [illegible]

Your Excellency's assumption that the ciphers assigned to [illegible] of this office to be sufficiently secure, is correct. The Foreign Office still takes the point of view that the other ciphers [illegible] the [illegible] according to [illegible] as long as there is no betrayal [illegible] or [illegible] compromised [illegible] likely [illegible] change [illegible] Unfortunately it has not been [illegible] in Madrid [illegible] change in [illegible].

As the [illegible] of the Foreign Office [illegible]

[illegible] (Signed) [illegible]

To the Chief [illegible]
General of [illegible]
No. [illegible]

TOP SECRET

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

19

TICOM/D-78

TOP SECRET

PROPOSED COLLABORATION BETWEEN GERMAN FOREIGN OFFICE AND ARMY

The attached translation from Ticom document T.165 was received from A.S.A. Washington.

2. T.165, from the files of Section Pers Z.S. of the German Foreign Office, consists of Diplomatic Memos (1944) on proposed joint working by the German Foreign Office and Army on Russian Cyphers.

Ticom
30th September, 1946.

No. of Pages: 4

Copy No: 6.

Distribution:-

L.S.I.C.

1. T
2. S
3. H and M
4. L
5. E
6. H.71
7. H.62
8. H.63 for Dr. G.W. Morgan
9. L-91
10-13 Ticom Files

U.S.

14 U.S.L.O.
15-18. Op-20-G
19-22. A.S.A.
23. Director, A.S.A. Europe) via U.S.L.O.

T. 165. (Proposed Collaboration between Foreign Office and Defense)

Berlin 23 II 34.

My dear Mr. Superior Government Counsellor:

One could begin with the taking over of our F 65 (328) Monday if you find the following lines acceptable.

For the present we could be ready for this purpose Monday, Tuesday, and Wednesday from 3:45 to 6:00 p.m.

Respecting the other numbers 49, 50, 53, 54, I shall phone you further suggestions early on Monday.

Respectfully yours

Dr. Müller

On 19 II Capt. Oschmann called on me to talk over with me technical details concerned in (our proposed) collaboration.

In the course of the conversation he mentioned an utterance by his chief, Corvette Capt. Patzig. to the effect that all cryptanalytic connections with F.A. should be dropped since Cryptanalytic work did not belong in the province of F.A

Details of the collaboration were then drawn up in broad outline.

Berlin, 19 Feb. 1934

Draft.

This forenoon Capt. [illegible], Prof. Nowopaschenny, and ORR Fenner of the cipher bureau of the Reichswehr (Defense) came to the (Foreign) Office to talk over the possibilities of technical cryptographic cooperation in the field of Russian ciphers.

To my great disappointment I learned that the gentlemen from the Reichswehr were not able to give any suggestions whatsoever in the field of Russian ciphers and that since 1930, when I last talked with them, they had had absolutely no success with Russian ciphers on foreign circuits. Mr. Fenner summed this up with the words: "Comlletely blank." The Reichswehr has only worked on Russian army, navy and GPU ciphers employed in internal radio traffic and intercepted here. This material has not been available to us; it has been sent us only in exceptional cases, evidently by mistake. The work of the Reichswehr on this material has yielded practical results. Prof. Nowopaschenny informed me briefly that for cipher messages of the GPU in internal traffic a 5-place code is used, the first and second [illegible] with changing substitution tables which [illegible] [illegible] military or naval [illegible] work to obtain [illegible] men of the Reichswehr [illegible] Novopaschenny and [illegible] ciphers. I pointed out [illegible] between the ciphers [illegible]

Everywhere there are systematic codes and extensive additive recipherments. I recommended working in the field of least resistance and made the following concrete proposal: To study fully in a statistical fashion the Strahlen-Verfahren (ray-system) Wn. Bl. A. 1. in use between Berlin and Moscow up to 31 Dec. 1930 while the 5-place Wn. T. C. II. was still employed and on which many preliminary studies are at hand. I hope through such statistics to be able to investigate the Tritheims already discovered with regard to further occurrences, i.e. to determine whether the quota of repeats of the Tritheim lies higher than 2 or 3. I showed the gentlemen from the Reichswehr the strikingly frequent repeats of the Tritheim keys and handed Prof. Nowopaschenny 26 sheets with the "Tritheim fragments" of Wn. Bl. A. He promised to have these sheets copied as quickly as possible and to send me a copy.

(Signed) Paschke.

In a conversation between Capt. Oschmann, Capt. Weiss, and myself in the R. W. M. on 12 II 34 the following suggestions for collaboration by the cipher sections of the army and the Foreign Office were made in view of a possible mobilization: Exchange of experiences and greatest possible cooperation in the field of

1. intelligence technique
2. cryptanalysis
3. our own cryptographic service.

Re 1.: To assure undisturbed communication with offices abroad both the A. A. (Foreign Office) and R. W. M. (Reichswehrministerium) should work to set up radio communication agencies quite independent of foreign means of communication.

In the A. A. this should include advising the missions in the procurement of commercial broadcast receivers and as far as possible supplying the same from the central office.

The R. W. M. on the other hand lays special emphasis [illegible] placed on setting up in at least part of the places apparatus which will ensure the widest possible telegraphic reception and for very special occasional purposes a potential, camouflaged sending station. Insofar as military attaches are stationed with missions the R. W. M. would, in agreement with the A. A., equip such receiver/sender stations and supply the attache a technically trained man to operate the same. In the opinion of the R. W. M. it would be most useful for the A. A. to equip other posts with such apparatus and to supply a civilian operator.

Re 2.: Since the traffic of the European countries is worked on by R. W. M. in preparation for any possible emergency and by the A. A. for current information, closer cooperation in this field has decided on. In the interest of the most rapid possible increase in production and to avoid duplication it is the intention--after exchange of information on the present status of the work of both parties--to make a division of work on current systems and to form common workgroups for the unsolved political and military systems, on which the A. A. in particular has [illegible]

been able to work due to lack of personnel. Details are to be settled in conferences of the section heads.
Re 3.: Since the army with its military attaches is dependent for transmission of its reports upon the cipher systems of the A. A., it has a departmental interest in the security of the diplomatic systems. It was suggested that close cooperation would be in the mutual interest in the matter of defense against foreign interference, in exchange of agent's information on the subject and regarding breaches of security in the handling of the ciphers.

PUBLIC RECORD OFFICE

Group/Class HW 40

Piece 181

TICOM/I-172 retained under S3(4)
of the PRA 1958

(date) 11/2/2004

(Signed)

OFFICES OF THE CYPHER POLICY BOARD,
C/o ROOM 17,
FOREIGN OFFICE, S.W.I.

10, CHESTERFIELD STREET,
LONDON, W.I.
GROSVENOR 3095-6

15(Q) (1)

TOP SECRET

Ref. [illegible] 1983 28th September, 194[illegible].

Dear Dudley,

Herewith two copies each of interrogations of Fraulein Hagen and O.R.R. Paschke.

I have not copied your questionnaire for Hagen as I take it you have retained a carbon. I assume also that you will arrange for any necessary circulation by the Ticom Committee.

Yours sincerely,

Cdr. (S) R. Dudley Smith, R.N.
Station 'X'

Encs.

PUBLIC RECORD OFFICE

Group/Class HW 40

Piece 181

Interrogation of Fräulein Haggen retained under S3(4) of the PRA 1958

(date) 11/2/2000

(Signed)

This is a COPY
The original has been
retained under
Section 3(4) of the
Public Records Act

Interrogation of O.R.R. Adolf Paschke, (Berlin-Wilmersdorf, Johannisbergerstrasse 17a) of Pers Z, by Commander Bull, U.S.N.R., at Military Government Offices, Marburg Lahn, Germany.
15th September, 1945.

16

---

1. Paschke worked as a cryptographer for the German Army 1915 - 1919. Joined Pers Z 1919. Joined Nazi Party 1933.

2. Selchow (Director Pers Z) as a rule dealt direct with Ribbentrop and did not go through Schroder and/or Weiszacker.

3. The instructions from Ribbentrop were invariably of a general nature and solely concerned with the subject matter of intelligence - e.g. Poland - or the invasion. He did not concern himself with the details of different systems in any way.

4. Ribbentrop was well aware that the more important intelligence could only be gained from attacking the recyphered systems, but he was apparently satisfied not to press for the additional staff which would be required and contented himself with the material obtained from the single process codes.

7. They worked on all traffic - Embassies, Legations and Consulates.

8. He thinks the O.K.W. had the biggest staff - about 400. None of the other bureaux had more than 300.

9. Ribbentrop only read about 20% or 30% of the material produced. His secretaries, e.g. Herr Weber and Herr Loesch selected these for him.

10. F.A. read I.D. for a short time in summer 1941.

11. Ministerialrat Fenner (believed in Bavaria) (in 1944 O.R. Wendland assisted him) - held the same position in O.K.W. as Paschke in Pers Z and was a good friend of his, both being born in St. Petersburg. His (Fenner's) immediate chief was Oberst Kettler and his (Kettler's) was General Gimmler, then Keitel.

12. In F.A. Ministerialdirigent Schroder held the corresponding position to Paschke. Ministerialdirektor Schapper was above him and then Goering.

13. The German secret cypher systems Paschke believed to be first class.

14. O.R.R. Langlotz was head of department of Auswartiges Amt dealing with German cyphers.

15. In 1944 O.K.W. (Fenner) took over the organisation of O.K.W., O.K.L. and O.K.H. cypher construction.

16. Paschke considers that of the three high officials

/continued

concerned with diplomatic traffic von Ribbentrop took most interest as had von Neurath before him. The most interested of all was von Rathenau (1922).

17. The reading of code telegrams besides giving occasional 'highlights' provided a wealth of press material not otherwise available.

18. The Staatssekretar decided on the distribution of telegrams in the A.A.

19. All the Pers ZS papers (40 chests) believed to have gone south to Bavaria from Muhlhaus in mid-April 1945. There were no other copies left.

20. Individual texts bore no marking but the files and folders were marked Geheime Reichssache.

21. No attack was ever attempted on British Attache Cyphers. They were considered O.K.W.'s "pigeon."

22. Paschke was in practice the "Cypher Security" Adviser for the A.A.

23. Frau Paschke worked in Dr. Paschke's section for three years, but only as a clerk. She has never been asked by the Russians (from whom she obtains permits to visit Paschke from Berlin to Marburg) what she did or what her husband's profession was. Paschke enquired as to the possibility of the British providing air transport for Frau Paschke to join him at Marburg.

E(a)

Sent 23/11

[illegible]

13

[illegible]
[illegible]

Attached are [illegible] of three documents from [illegible] of [illegible] Foreign Office at [illegible].

(a) Short [illegible] report [illegible] the [illegible] ([illegible]).

(b) [illegible] report on [illegible] development of the [illegible]

(c) [illegible] of [illegible] cypher [illegible] by [illegible] German Foreign Office for [illegible] dated 5/12/[illegible]

(TICOM Docs. [illegible] and 16).

[illegible]   No. of Pages: [illegible]

30th October, 1945

DISTRIBUTION

British

[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]

U.S.

[illegible]
G-2 (via Lt. Col. [illegible])
[illegible] (5) (via Major [illegible])
[illegible]
[illegible]
[illegible]

[illegible]

Chairman
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]

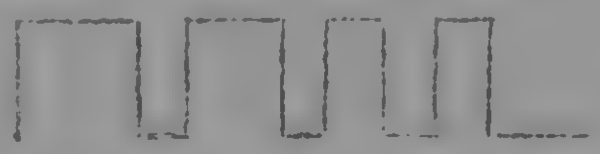
[illegible]

[illegible]
D.D. ([illegible])
A.D. ([illegible])

Notes on Modern Wireless [illegible] Apparatus

For receiving messages sent out, there are available today a number of instruments all functioning on more or less like principles. If it is a question of taking Morse characters at a speed up to 175 a minute, then it is generally by headphone and typewriter. The German telegraphers send their Morse at an average of 25 words, i.e. 125 letters per minute since a word averages 5 letters. English and American stations work at a speed of 30 to 35 words, i.e. up to 175 letters per minute. Since auditory reception usually runs for hours at a time and may be rendered very difficult by local disturbances, fading, or jamming, it naturally calls for a great amount of practice and great concentration.

At a speed of more than 175 letters per minute, such as is attained with mechanical transmitters, in simple cases a Morse printer is used or better yet a lever writer /Hebelschreiber/ or recorder devised especially for this purpose and successfully employed for years in commercial communication. The principle of operation is briefly: In the field of a powerful electric magnet is suspended in vertical position by two thin wires a revolving coil to which the impulses are conducted when received, amplified and rectified by the radio receiver. At the upper end is a small, horizontal silver tube one end of which is immersed in a small inkwell while the other end traces a colored line on a paper tape which is moved past by a motor. As this coil receives short or long impulses it is diverted from its rest position to one side and the tube traces the impulses in a jagged line. The letter Z would, for instance, appear as follows:



Such a device, given good conditions for reception, permits of a speed up to 1250 letters per minute.

In recent years another instrument has become increasingly important. This is the Morse-printer of Siemens-Hell which prints Morse signals as follows:

(Line of tape - no sample available.)

Its advantages are: simple, sturdy construction and relatively simple operational attention. Speed attained is about [illegible] letters ([illegible] words) a minute.

[illegible] speed [illegible] machine reaches as high as [illegible] letters a minute. This performance is achieved by making the movable element of the magnet very light and [illegible] few tenths of a millimeter.

It has long been the ambition of technicians and engineers to build a machine which would permit direct transmission of the printed letter by radio as the teletype does by cable. To date the only machine giving tolerable results when reception conditions are good is the SH-Hellschreiber /teleprinter/ invented by graduate engineer Dr. Hell some time ago and constantly improved. It permits a speed of 300 words a minute.

Formation of the characters is as follows: The radio receiver amplifies and rectifies the impulses received. When such an impulse comes in, the receiving magnet attracts its anchor, the edge of which presses a paper tape, which moves at uniform speed, against the writing spiral which is mounted on a rapidly revolving cylinder and inked by a felt inking roll. Thus there is printed on the tape a vertical stroke with interruptions corresponding to pauses between impulses, which together yield the form of the letters which appear as follows:

One may, therefore, regard the Hell-system as a simple transmission of the printed letter by facsimile.

****

Translated by Dr. Ray W. Pettengill
10 August 1945

15-7-44
Ticom 380

TOP SECRET

S.F.B. Morse and the Morse Code

by Assistant Paula Mueller (née Rhode)

A. Historical Survey.

The Morse code is a system of symbols serving for transmission of information by electric current, light, etc. Knowledge of it is useful not merely for radio and telegraph operators, etc., but for everyone who has much to do with telegrams, chiefly because this will give clues for correcting garbles.

In olden times people relied on swift courier service, then sound and light signals were employed. The fact that water conducts sound better than air was known in Aristotle's day (ca. 500 B.C.) so that it is likely that underwater signals were used at that time.

Not until recent times do we find purely technical solutions of the problem of speeding news from place to place. The best known arrangement is the telegraph introduced by the Frenchman Chappe in 1793 under Napoleon. This involved light signals at night and shadows by day. While it has been calculated that the torch telegraph communication of the Greeks could send up to 173 signals in a half hour, Chappe's telegraph required only 11 minutes for the same number of signals. With later improvements, in particular in the form used in 1813 in Prussia on the line Berlin - Coblenz, this speed was materially increased. The distance between the individual telegraphs (the position of the arms and beams was observed by telescope) averaged 14 km. Some idea of the value of the telegraph service of those days may be gained from the fact that a signal took only two minutes to travel from Paris to Lille (200 km).

Chappe's telegraph brings to an end an epoch characterized by imperfect, time consuming transmission of news. But even though the speed of Chapee's telegraph was great for his day, its general use was impossible due to costs. Since at least two officials had to be present at every relay station, a telegram from Berlin to Coblenz required the activity of 122 officials, an outlay which very few telegrams would seem to justify, and which was all the more a luxury since only for a few hours of the day was visibility adequate for reading the pointer positions. It is interesting, however, that Chappe's telegraph is still used on railroads and for regulating traffic.

Chappe's telegraph in its various transformations was the direct precursor of the electric telegraph. With electricity the bearer of the news becomes a [illegible] which moves with tremendous speed compared to the light waves previously employed, and with [illegible] which, compared [illegible] light, is [illegible]

The first electric telegraph writing permanent symbols was put in operation in Munich in 1837 by Steinheil. In that same year Morse made a preliminary announcement concerning his invention to the United States Patent Office.

To Morse belongs the credit for having so far developed his invention that due to its advantages it could win world wide acceptance. In the Morse telegraph electric impulses of longer or shorter duration call forth corresponding movements of the anchor of an electric-magnet; these movements activate the writing lever which writes characters in shorter or longer strokes on a paper tape which is moved past at uniform speed.

1. The Structure of the Morse Alphabet.

To Morse we owe a carefully thought out arrangement of such short and long telegraphic elements (impulses) to form an alphabet which has now found international recognition. On the paper these elements appear as short and long black strokes separated by white intervals. The short stroke is the unit of length and is termed "dot" /Punkt/. The long stroke is thrice as long and is termed "dash" /Strich/. Dot and dash are the elements.

The pause between the elements of a Morse signal has the length of one unit (one dot); the pause between the Morse letters of a word has the length of three units; the pause between two words the length of five units. (In our representations these lengths have not been observed exactly.)

The black unit of length (dot) and the white unit of length we call the "basic elements" /Grundelemente/.

A Morse text can be represented as a dyadic sequence of the two basic elements: if we call the white element 0 and the black 1, the Morse text

.-.   .   ..   .-   -...
r   e   i   s   e   a   b

takes the form: $\underbrace{1011101}0\underbrace{1}00\underbrace{101}00\underbrace{111}00\underbrace{1}000\underbrace{10111}00\underbrace{111010101}$

r   e   i   s   e   a   b

Dyadic sequences of various types play an important role in mathematics and cryptology.

A second manner of representing a Morse text by zeros and ones would be to represent the dots by 0, the dashes by 1, keeping the intervals between elements and words as genuine intervals:

010   0   00   000   0   01   1000
r   e   i   s   e   a   b

But this is no longer a dyadic text, rather we must conceive it as a 30-adic text. The text elements are the 30 variations of 1 - 4 zeros and ones.

In table 1 the Morse alphabet is given in its present form. As a matter of principle in the Morse alphabet the most frequent letters are represented by the shortest symbols. Table 1 contains in addition to the 26 letters of our alphabet ä, ö, ü, ch, thus exhausting the 30 Morse symbols with 1 - 4 elements.

In table 2 the Morse alphabet (without ä, ö, ü) is represented by mnemonic words. These are intended to facilitate memorizing the Morse letters. The first letter of the word corresponds to the letter, the number of syllables to the number of dots and dashes, each syllable with "a" is a dot, any other vowel means a dash. For the letters j, q, y, ö note the word jyqö: In the Morse symbols for these the dot moves ahead corresponding to the position of the letters in the word:

j = · — — —

y = — · — —

q = — — · —

ö = — — — ·

Tables 3-7 also serve to aid in memorizing Morse letters. But if you really want to fix a Morse letter, its rhythm must become a part of you.

a = d e d a a

b = d a a d e d e d e

c = d a a d e d a a d e etc.

Two Morse letters are termed symmetrical with respect to one another if one arises from the other by reversing the order. A Morse letter is called symmetrical within itself if reversible. In table 3 pairs of symmetrical Morse letters are listed.

Two Morse letters are termed dual if one arises from the other by replacing dots by dashes and dashes by dots, see table 4. In table 5 (figure of a cross) the Morse letters are arranged as follows:

In the left half stand those letters beginning with a dot, in the right half stand those beginning with a dash.

In the upper half are those ending in a dot, in the lower half those ending in a dash.

From one Morse letter a cycle may be generated by cyclic substitution of the elements. One writes a Morse letter, then the one arising when the last element is transposed to the beginning, etc.

Those Morse letters which consist of only one type of element form a cycle of their own. Table 6 shows the cycles of Morse letters.

The Morse reading table /Ablesetafel/ (Table 7) serves for taking down Morse messages. When sending is slow it can be used without previous memorizing of the letters. It is intended chiefly to facilitate learning the letters.

The reader follows the letters given as dot or dash starting at the top center. If the first element is a dot, he reads off the left half, if a dash off the right half. If a dot follows, he follows the dotted line, if a dash follows he takes the solid line. When the letter is completed he reads the letter which he has reached.

In table 8 are Morse symbols for numbers, in table 9 those for foreign letters, punctuation, and procedure. Table 10 gives the American, table 11 the Japanese, and table 12 the Russian symbols used for domestic traffic.

It is important for anyone who has much to do with telegrams to learn to recognize the possible garbles.

C. Investigation of Possible Errors.

In the telegraphic transmission of a text there are in general three different types of errors. Almost always they result from imperfect work of the telegrapher:

a) A dot is confused with a dash or vice versa, thus

a . _ with . . i

e . with _ t

i . . with . _ a

n _ . with . e

t _ with . e

b) Omission of a dot or a dash;

h . . . . s

m _ _ _ _ _ o

In [illegible] confusion of [illegible] often.

c) Bad spacing:

mm [illegible] and [illegible] etc.

ot [illegible] and [illegible] etc.

to [illegible] and [illegible] etc.

Individual letters may be [illegible] as follows:

[illegible]

ken [illegible] etc.

To correct these errors one must keep the Morse alphabet in mind.

6. Life of Morse.

Samuel Finley Breese Morse was born 27 April 1791 the eldest son of the Reverend Jedidiah Morse, known for his Geography of America, in Charlestown, Massachusetts. He studied for a time, then devoted himself to painting. He made several trips to Europe for study. On board the sailing vessel "Sully," which left Le Havre on 1 October 1832 for America he met Dr. Charles Jackson, Professor at Harvard College, who gave him the inspiration for [illegible]. Back in America to work on painting, in 1835 he was appointed Professor of the Literature of the Pictorial Arts at the [illegible]. In the same year he displayed at New York University the model of a telegraph [illegible]. However, [illegible] in 1837 he [illegible] the patent with the first recording telegraph. [illegible] in 1843. He was given [illegible] for an experimental line between Washington and Baltimore. In [illegible]. He died in 1872.

[illegible]

Philadelphia claimed at a session of the French Academie in 1865 the formation of an alphabet of dots and dashes as his invention, basing his claim on a work published in 1829. The form of the alphabet used by [illegible] Bain with the apparatus he patented in 184[illegible] was a modification of this, and this was in turn adopted by Morse with unimportant modifications, and has later undergone some further minor changes to reach its present form.

[illegible]

[illegible] 1

a	.-	k	-.-	u	..-
b	-...	l	.-..	v	...-
c	-.-.	m	--	w	.--
d	-..	n	-.	x	-..-
e	.	o	---	y	-.--
f	..-.	p	.--.	z	--..
g	--.	q	--.-	ä	.-.-
h	....	r	.-.	ö	---.
i	..	s	...	ü	..--
j	.---	t	-	ch	----

* [illegible]

TOP SECRET

Table 1.

[illegible]

[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]		[illegible]
[illegible]	[illegible]	
[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]
[illegible]		[illegible]
J	Jahrestunde	[illegible]
[illegible]	[illegible]	[illegible] Schweden
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	

[illegible]

[illegible]

TOP SECRET

Table 1

Pairs [illegible]

a	. —	— .	n
b	— . . .	. — — —	j
c	— . — .	. — . —	ä
d	— . .	. — —	w
e	.	—	t
f	. . — .	— — . —	q
g	— — .	. . —	u
h	. . . .	— — — —	ch
i	. .	— —	m
k	— . —	. — .	r
l	. — . .	— . — —	y
o	— — —	. . .	s
p	. — — .	— . . —	x
v	. . . —	— — — .	ö
z	— — . .	. . — —	ü

[illegible]

TOP SECRET

[illegible]

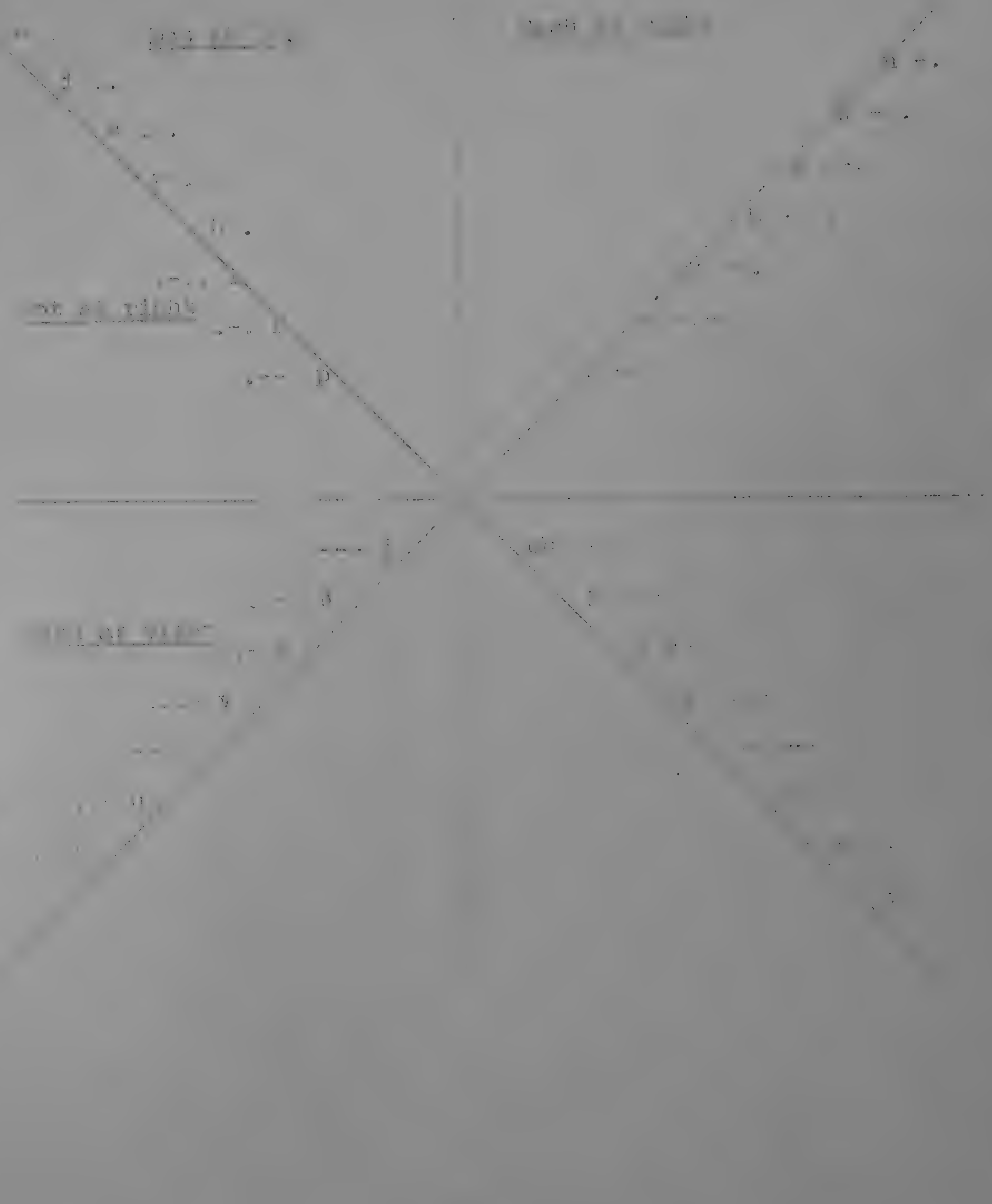
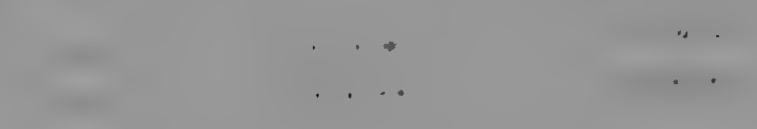


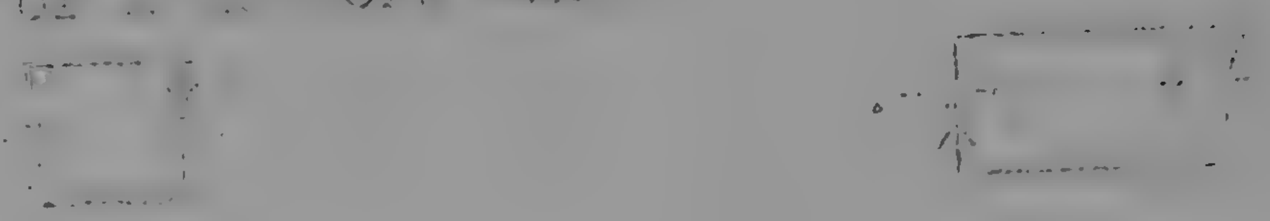
Table 5

Cycles of [illegible] Letters

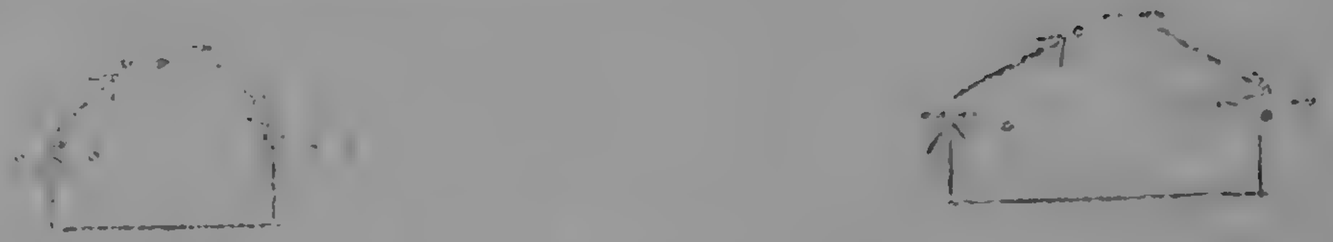
1. Of the following 8 letters each forms a cycle of its own consisting only of dots or dashes:



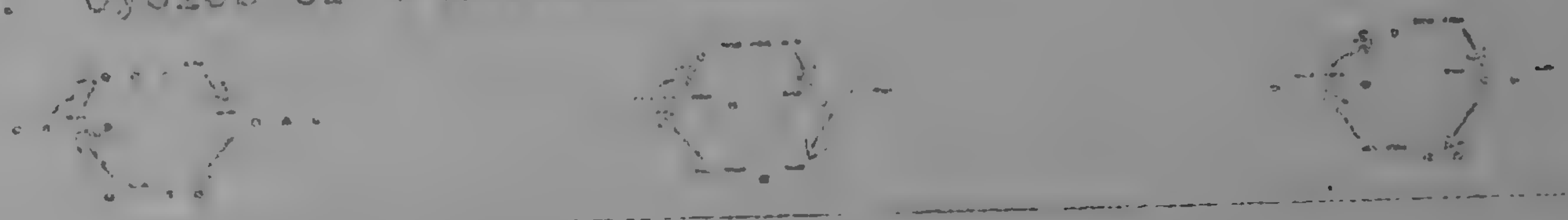
2. Cycles of 2 letters each:



3. Cycles of 3 letters each:



4. Cycles of 4 letters each:



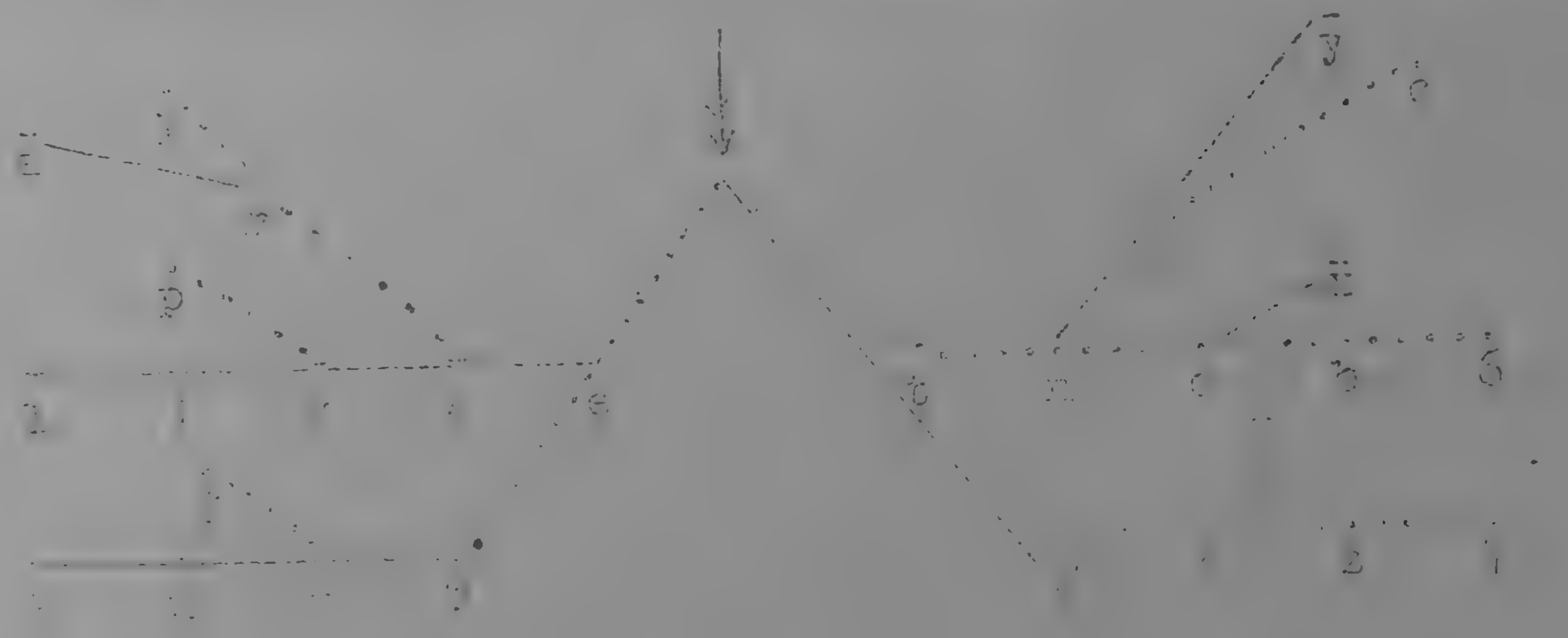


Table 3

Numerals			Abbreviated Numerals	
1	[illegible]	1	[illegible]	a
2	[illegible]	2	[illegible]	u
3	[illegible]	3	[illegible]	v
4	[illegible]	4	[illegible]	[illegible]
5	[illegible]	5	[illegible]	[illegible]
6	[illegible]	6	[illegible]	[illegible]
7	[illegible]	7	[illegible]	[illegible]
8	[illegible]	8	[illegible]	[illegible]
9	[illegible]	9	[illegible]	[illegible]
0	[illegible]	0	[illegible]	[illegible]

Table 4

[illegible]	[illegible]	Question mark (?)	[illegible]
[illegible]	[illegible]	Apostrophe (')	[illegible]
[illegible]	[illegible]	Dash (-)	[illegible]
[illegible]	[illegible]	Diagonal (/)	[illegible]
[illegible]	[illegible]	Parentheses ( )	[illegible]
[illegible]	[illegible]	Open and close quote (" ")	[illegible]
[illegible]	[illegible]	Underline [illegible] and [illegible] passage to be underscored	[illegible]
[illegible]	[illegible]		
λ	.--.-	Message beginning	-.-.-
Ŧ	--.--	Equality sign (=)	-...-
Period (.)	[illegible]		
[illegible]	[illegible]	[illegible] between letters and numbers in mixed text Example: 25 a 1 = 25 .-..- a .-..- 1	.-..-
Comma (,)	[illegible]		
Colon (:)	---..		

Table 9 (Cont'd)

I understand	...-.
Error	....
Cross	.-.-.
Start sending!	-.-
Wait!	.-...
End of traffic period	..-.-

Table 10

American Morse (Domestic Traffic)

		Frequent errors:	Numerals:		Frequent errors:
A	.-	i,f,c	1	.--.	p
B	-...	d,h,ts			
C	.. .	s,z,ie	2	..-..	5
D	-..	b,ti			
E	.	t	3	...-.	4
F	.-.	r,t,en			
G	--.	n,c,ne	4	....-	5
H	....	s,p,z,y,es			
I	..	s,i,e	5	---	
J	-.-.	c,k,kn			
K	-.-	j,n,te	6	......	p
L	⸺	t,n			
M	--	n,a,t	7	--..	
N	-.	o,t,te			
O	. .	n,i,ee	8	-....	
P	.....	h,s			
Q	..-.	f,g,[illegible]	9	-..-	L
R	. ..	[illegible]			
S	...	h,v,i	0	⸺	L
T	-	l,[illegible]			
U	..-	v,[illegible]	Period	..--..	
V	...-	u,[illegible]			
W	.--	[illegible]	Comma	.-.-	
X	.-..	[illegible]			
Y	.. ..	o,c			
Z	... .	h,e[illegible]			
&	. ...				

Table 11

Japanese Syllabic (Domestic) Traffic

	a	i	u	e	o
	a --.--	i .-	u ..-	e -.---	o .-...
k	ka .-..	ki -.-..	ku ...-	ke -.--	ko ----
s	sa -.-.-	shi --.-.	su ---.-	se .---.	so ---.
t	ta -.	chi ..-.	tsu .--.	te .-.--	to ..-..
n	na .-.	ni -.-.	nu	ne --.-	no ..--
h	ha -...	hi --..-	fu --..	he .	ho -..
m	ma -..-	mi ..-.-	mu -	me -...-	mo -..-.
y	ya .--		yu -..--		yo --
r	ra ...	ri --.	ru -.--.	re ---	ro .-.-
w	wa -.-	(w)i .-..-		w(e) .--..	wo .---

n .-.-.

[illegible] sign .. Example: [illegible]

[illegible] sign ..--. Example: [illegible]

[illegible]

T O P   S E C R E T

Table 12

Russian Morse (Domestic Traffic)

а	.-	к	-.-	ф	..-.
б	-...	л	.-..	х	....
в	.--	м	--	ц	-.-.
г	--.	н	-.	ч	---.
д	-..	о	---	ш	----
е	.	п	.--.	щ	--.-
ж	...-	р	.-.	ы	-.--
з	--..	с	...	ь	-..-
и	..	т	-	ю	..--
й	.---	у	..-	я	.-.-

[illegible]
[illegible]

TOP SECRET

T[illegible]6

Amt.Ausl./Abw....

Abw................../II

Stahnsdorf, 5.12.40.

To

Foreign Office

Att.Reg.Rat.[illegible]

In the inclosed document is sent an introduction to the use of cipher machine and the placement positions of the following offices abroad:

1.	Adolf: Anton Karl	4th and 9th group
2.	Benito: Anton Emil	1st and 5th group
3.	Bernhard, Emil	4th and 8th group
4.	Berta: Fritz	2nd and 11th group
5.	Ida: Anton Dora	2nd and 6th group

The first four letters of the above groups form the message key, while the fifth letter is a null and is not to be enciphered.

1. Inclosure

Instructions for Keys

Basic information concerning keys:

For enciphering with the cipher machine, there are, of necessity a) daily keys, and b) message keys.

a) The daily key changes daily at 0000 hours and is a special one determined by schedule. It consists of an internal and external setting.

To the internal setting belong wheel arrangement and Ringstellung. The wheel arrangement is the order in which the separate wheels are placed in the cipher machine from left to right. The left wheel remains fixed, so that three wheels can be changed.

The Ringstellung is the placement of the letter-ring (tire) on the cipher wheel.

Example: The Internal Setting

	Wheel Arrangement		Ringstellung
I	III	II	[illegible]

[illegible] that the cipher wheels I, III, II are to be placed from left to right [illegible]

The Ringstellung:	[illegible] to the letter [illegible]
wheel I	[illegible]
wheel III	[illegible]
wheel II	[illegible]

The [illegible] setting is read [illegible] [illegible] of the cipher machine from left to right, and is designated in the [illegible] of the basic setting (Grundstellung). It is used only for the formation of the indicator groups.

Example: Internal setting (Grundstellung): This means that the four cipher wheels have each been turned so that, reading from left to right, the letters [illegible] appear in the four windows.

[illegible] The message key is a four letter group which is to be set, from left to right, in the windows, through the [illegible] and displacement of the [illegible] on the message setting. The message key is chosen by the cipherer at random and is transmitted [illegible] enciphered in the indicator groups. [illegible] it must be [illegible] [illegible] indicator groups. [illegible] telegram, a different message key must be chosen.

Indicator groups: Each enciphered message contains two indicator groups in which the enciphered message key is contained. The indicator groups proper are four letters long, the fifth letter of the group concerned (in which the indicator group is found) is a null and will not be typed out. When the typing out of both indicator groups, the daily key will be given twice. Naturally, the two indicator groups must not be enciphered again with the text groups.

Enciphering: Set the daily keys. Choose and type out the message key. Form the indicator groups and insert them into their proper places in the message. Using the message key as the basic setting, type out the text of the message and enter the letters which light up as five-letter groups.

Deciphering: Set the daily keys. Strike out the last letters of the indicator groups, and type out the indicator groups. Set up the resulting message key. Type out the five-letter message groups and read the clear text from the letters which light up.

Trans. by Lt. M.C.Lane,
Aug. 1945

This is a copy
The original has
been retained under
section 3(4) of the
Public Records Act
1958.

Form R.1.—February, 1932.
Revised, November, 1939).

MINUTE SHEET.

CX .. /1862
Source
No. 14
Date

DISTRIBUTION

V.G.

Ref. Dudley-Smith's letter DS/1019/1419 27.8.45 on Harold KIRFEL.

K.'s W.R. case officer has been asked to ensure that KIRFEL is given an opportunity of saying what he knows of Japanese Codes and Cyphers, though I think he was probably more of a language than a cypher expert.

I enclose a copy of the paragraph dealing with Japanese Secret Communications from the Tactical Interrogation report JZX 1860 (OSS SCI Rome) 2nd August 1945, and will of course let you know the results of his 020 interrogation.

Will you let us have any further questions for KIRFEL, unless you prefer to wait until you have seen his 020 report?

V.F.10
18.9.45.

ACTION PROPOSED

Copy

C. Japanese Secret Communications.

6. In November 1944, Subject's section of Abt VI obtained the Manchurian code through agent Alla MEYER, chief secretary of the Manchurian Embassy who took the code out of the Embassy safe and put it back after it had been photographed. One photostat was kept with Amt VI and another was handed over to OKW-Chi (Chiffrierabteilung), directed by the mathematician Dr. HUETTENHEIM. The Japanese expert of OKW-Chi was first Lt. Dr. ADLER (about 32 years old, 1.70 m, oval face, youthful intelligent expression, possibly to be located through Assessor TROMEL, secretary of the German-Japanese Society, Berlin, Ahernstrasse 1 or 2).

7. The Code consisted of abook about 300 pages with an introduction in Japanese and divided into an encoding and decoding section. It contained numbers of 4 digits from 0000 to 9999 (or 8888), and to each number corresponds a Japanese sign standing either for a word or for a grammatical form of a noun, verb, etc. As the coded messages of the Manchurian Embassy consisted of groups of 5 numbers, however, some additional operation was necessarily involved after the encoding had been done according to the book and Dr. ADLER was unable to find the solution to this problem.

8. While messages of the Manchurian Embassy were sent in groups of 5 figures, those of the Japanese Embassy consisted of groups of 5 letters. Subject believes, however, that the two systems were not entirely independent from each other and that the Japanese system too was ultimately based on the code stolen from the Manchurian Embassy.

9. Code-clerk in the Manchurian Embassy was a Japanese called KASAI. He should be fully informed about all technicalities connected with encoding and decoding.

10. A cypher machine was kept in the private apartment of the Manchurian Embassy councillor EHARA. According to subject, the Japanese cypher machine is fundamentally different from all other cypher machines in use.

11. Messages from Berlin to Tokyo went via Harbin, messages from Tokyo to Berlin via Madrid.

This is a copy
The original has
been retained under
Section 3(4) of the
Public Records Act
1958

TOP SECRET

[illegible]/15[illegible]/[illegible]

13

Major Mason, Section V.

(Through Section V C).

Reference CX 1862 of 30/4/45. The following are the questions we should like put to [illegible]. The paragraph references are to the interrogation report [illegible] 1900.

(1) What success did German cryptanalysts have with Japanese systems?

Para 6 :-

(2) What other Japanese crypto materials were lifted ?

(3) Was all cryptographic material lifted by Amt VI passed to [illegible] and was any other cryptographic organisation provided by Amt VI with such material ?

Para 8 :-

(4) What reason has [illegible] for thinking that Japanese and Manchurian cipher systems were not independent ?

(5) Why should he think the Japanese system was based on the Manchurian ?

(6) When he speaks of the 'messages of the Japanese Embassy', does he seriously suppose all messages to have been in the same system ? How did he obtain access to Japanese cipher messages emanating from Berlin ? (By intercepts, photographs of telegrams, etc. ?). What amount did he see ? What would be his estimate of the bulk of cipher traffic sent by the Japanese in Berlin per day (or month or year) ?

Para 12 :-

(7) Describe fully the Japanese [illegible] machines. Could anyone read the machine messages ?

Please turn over

(8) With what other cipher machines is he acquainted ?

(9) Was this machine used, or just stored in [illegible]'s apartment ?

[illegible] September, 1945.

Copy to :-

Mr. F.A. Kendrick.
Major J. Seaman.
Ticom Duty Officer.

TOP SECRET U.

To: Commander Dudley Smith, Station X. (12)

From: Mr. F. A. Kendrick, Berkeley Street.

Date: 26th September, 1945.

Interrogation of KIRFEL.

I append Thornett's suggestions. K. might also be asked if all cryptographic material lifted by Amt VI was passed to OKW/Chi and whether any other cryptographic organization was provided by Amt VI with such material. (9)

Judged from his recorded statements he does not seem likely to be a very fruitful or reliable source of cryptographic information.

F. A. Kendrick

Para.8 —

(4) What reason has Kirfel for thinking that Japanese and Manchurian cipher systems were not independent?

(5) Why should he think the Japanese system was based on the Manchurian?

(6) When he speaks of the 'messages of the Japanese Embassy', does he seriously suppose all messages to have been in the same system? How did he obtain access to Japanese cipher messages emanating from Berlin? (By intercepts, photographs or telegrams, etc?) What amount did he see? What would be his estimate of the bulk of cipher traffic sent by the Japanese in Berlin per day (or month, or year)?

Para.10 —

(7) With what other cipher machines is he acquainted?

(8) Was this machine used, or just stored in EHARA'S apartment?

Japanese [illegible]

TOP SECRET

Q DD/15(J)/1464

Mr. F.A. Kendrick

With reference to the attached documents, I would be grateful if Thornett, or anyone else concerned, could provide me with a questionnaire for KIRFEL.

Major Seaman has suggested the following questions :-

(1) What other Japanese crypto materials were lifted ?

(2) What success did German cryptanalysts have with Jap systems ?

(3) Describe fully the Japanese machine mentioned para 10. Could Germans read the machine messages ?

Would you please return the enclosures in due course with your reply.

R. Shacklane.
for Cdr. Dudley-Smith.

18th September, 1945.

Captain Thornett

What do you suggest ?

F.A.K. [illegible]/IX/45

Form R.1.—February, 1932.
(Revised, November, 1939).

MINUTE SHEET.

CX. 1862
Source
No.
Date

DISTRIBUTION

~~V.G.~~ 3/10
~~for~~
Cmdr. Dudley-Smith

With reference to your letter DS/1019/1419 of 27th August, the attached report on Dr. KIRFEL may be of interest to you, if you have not already seen it.

KIRFEL is now at Camp 020 and War Room have been instructed to have him interrogated on the question of Japanese codes and cyphers. However, as the interrogators have not been briefed on this subject, it would help a great deal if you could let me have some more specific questions to put to KIRFEL.

V.F.7.
30.8.45.

ACTION PROPOSED

This is a copy
The original has
been retained under
section 3(4) of the
Public Records Act

178

: COPIED IN WAR WOOM :
: DATE: 23-8-45 :

TOP SECRET

NO ACTION TO BE TAKEN ON THIS COPY

Memo: JZX-1860

2 August 1934.

To : SAINT, Washington
From : SAINT, Rome (BB008)
Subject : Tactical Interrogation of Dr. Harald KIRFEL
Reference : Our JZX-1647, dated 8 July 1945.

1. As a result of London's action on para 2 of our JZX-1647, this Unit was granted AFHQ permission to conduct a tactical interrogation of Subject.

2. In addition to clarification of questions arising in Plan CAESAR, Subject gave the following information on the JIS and on other personalities who should be priority targets for SCI Units in Germany and Austria.

TACTICAL INTERROGATION OF DR. HARALD KIRFEL

A. The Working of the Japanese IS in Germany:

3. The Japanese IS operated extensively in Germany through social and commercial contacts and conversations of the Japanese living in Germany and used many Germans as information channels without their direct knowledge. There definitely existed, however, also the paid agent type. The Axis situation favored the emergence of an intermediate type of agent who accepts gifts but is not on a regular payroll, as gifts were much more valuable in Germany than money and also because providing information for the Japanese ally was not considered treasonable.

4. Subject states that there were about 3,000 agents of the JIS operating in Germany. This included a great number of foreigners, such as Chinese seamen, White Russians, Poles, Indians, Czechs, etc. Among Germans, Subject has a specific suspicion against one German, Dr. Hermann LUFT, who maintained friendly relations with such Japanese as Dr. SATO and UCHIDA. Other possible Japanese agents known to Subject are:

a) Dr. OUCHIN, a White Russian girl who worked in the Manchurian Embassy. She might be also a Russian agent.

b) Miss ARENS, mistress of Gen. KONATZU and secretary in the Heereswaffenamt.

The Poles are said to have had important connections with the JIS. Subject states that NAKAGAWA, secretary of the Manchurian Embassy, played a "certain" role in the genesis of the WARSAW uprising of 1944.

B.............

B. Additional data on certain Japanese Personalities:

5.	a) Dr. SATO:-	Ministry Counsel, representative of the Japanese Ministry of the Interior in the Japanese Embassy, pro-Russian. Representative also of the Japanese Secret Field Police "KEMPEI" and one of his main tasks consisted in learning everything possible about German Gestapo methods. He was in direct contact with the Secret Service of the War Ministry. Secretaries: YOTSUMOTO and Miss KRUG (living in BERLIN-ZEPERNICK). Being pro-Russian, he decided to wait for the Russians with other Japanese civilians in BERLIN-BELITZ. Inner circle of SATO: Dr. MIYASAWA- dangerous individual, general helper for SATO. Dr. HARA- Asahi Shimbun representative. Dr. KATO - Nichi Nichi Shimbun representative.
	b) MAYEDA -	Studied in HEIDELBERG, is very educated. Pro-American. Member of the cultural relations section of the Embassy. Not believed to have had more than normal contacts with the Secret Service. Was lecturer of Japanese at VIENNA University 1944-45.
	c) MOTONO -	Anti-Russian, pro-Western democracies, anti-OSHIMA. Very rich and educated. His wife is half-French. A friend of LAVAL and well informed about the conversations between HITLER and LAVAL.
	d) KITAHARA -	Author of philosophical treatises. Directed an East Asia Institute in VIENNA and was in contact with the JIS for purposes of economic and technical espionage as well as an observer of political and intellectual currents in Germany. Is ultra-nationalist, hostile to practically every foreign country. Professor DONAT, teacher of Japanese at the Berlin University, knows him well.
	e) SUMA -	Japanese Ambassador in SPAIN - Chief of the Japanese Secret Service for Western Europe. Pro-Allied.
	f) ONODERA -	Japanese military attache in STOCKHOLM, pro-Russian, if not actually controlled by the Russians. Source of numerous items of information hostile to Germany.

C. Japanese Secret Communications.

6. In November 1944, Subject's section of Amt VI obtained the Manchurian code through agent Alla MEYER, chief secretary of the Manchurian Embassy who took the code out of the Embassy safe and put it back after it had been photographed. One photostat was kept with Amt VI and another was handed over to OKW-Chi (Chiffrierabteilung), directed

by the.........

by the mathematician Dr. HUETTENHEIM. The Japanese expert of OKW-Chi was 1st Lt. Dr. ADLER (about 32 years old, 1.70 m, oval face, youthful, intelligent expression, possibly to be located through Assessor TROMMEL, secretary of the German-Japanese Society, BERLIN, Ahornstrasse 1 or 2).

7. The code consisted of a book of about 300 pages with an introduction in Japanese and divided into an encoding and decoding section. It contained numbers of 4 digits from 0000 to 9999 (or 8888), and to each number corresponds a Japanese sign standing either for a word or for a grammatical form of a noun, verb, etc. As the coded messages of the Manchurian Embassy consisted of groups of 5 numbers, however, some additional operation was necessarily involved after the encoding had been done according to the book and Dr. ADLER was unable to find the solution to this problem.

8. While the messages of the Manchurian Embassy were sent in groups of 5 figures, those of the Japanese Embassy consisted of groups of 5 letters. Subject believes, however, that the two systems were not entirely independent from each other and that the Japanese system too was ultimately based on the code stolen from the Manchurian Embassy.

9. Code-clerk in the Manchurian Embassy was a Japanese called KASAI. He should be fully informed about all technicalities connected with encoding and decoding.

10. A cipher machine was kept in the private apartment of the Manchurian Embassy councillor EHARA. According to Subject, the Japanese cipher machine is fundamentally different from all other cipher machines in use.

11. Messages from BERLIN to TOKYO went via HARBIN, messages from TOKYO to BERLIN via MADRID.

D. Germans with knowledge of Japanese language and affairs:

12. Teachers of Japanese at German Universities:-

a) Professor Walter DONAT, Berlin University

b) Professor SCHARSCHMIDT, Berlin University

c) Professor KRESSLER, Bonn University, Bonn Clemensstrasse. Teacher of Subject.

d) Professor CLASSEN, Heidelberg University, scarce knowledge of language, expert on Japanese economy.

e) Professor Dr. SLAVIK, University of Vienna.

13. Colleagues of Subject at interpreter school, co-editors of military dictionary:-

a) Dr. Wolfgang HAENISCH, Berlin-Zehlendorf.

b) Dr. Frittjof SCHMELING, Berlin, Mommsenstrasse. Chemist.

14. Graduates from interpreter course:-

a) Clemens [illegible] - Wetzlar, merchant, has been previously in Japan for the BOEHLER steel firm.

b).........

b) Wilhelm BREITKREUZ, Berlin, Merchant, has been previously in Japan for the I.G. Farbenindustrie.

c) Ernst HANKOHL, architect.

d) von GLINZKY, 1st Lt. Assigned to Attacheabteilung OKW.

e) Hans KILB, Capt. Assigned to Attacheabteilung OKW.

f) Dr. von STECHOW, has knowledge of matters relating to Japanese Law, was together with Subject in charge of Far Eastern Division of the Int. Academy for Social and Administrative Sciences.

g) ARNDT, Capt., son-in-law of Generaloberst HARPE, Berlin-Wuensdorf, assigned to Attacheabteilung OKW.

h) Eduard FRISCH, engineer, Prague.

i) CLEMENT, fnu, Vienna.

j) Dr. MUELLER, Vienna or Tokyo.

k) Dr. FREUDENBERG, Muenchen-Haar.

l) KRAEMER, half-Japanese, Hamburg

m) Dr. SAEUBERLICH, Berlin

n) Ingeborg von GRONAU, daughter of the German Air Attache in Tokyo.

o) Eva KRAFT, Berlin, Kaminastrasse.

p) Dr. WALS, Berlin, assigned to the research department of the Air Ministry.

q) Dr. MIEBACH, Berlin, assigned to the research department of the Air Ministry.

r) BEUTHNER, half-Japanese, Berlin, assigned to the radio listening service of the Ministry of Foreign Affairs at the Seehaus, Berlin-Wannsee.

s) von SCHACK 1st Lt., Berlin, Attacheabteilung OKW.

t) Dr. SCHWINDT, Danzig, Technische Hochschule (Institute of Technology)

u) Major MOSSDORF, Berlin, OKW or OKL

v) HINDER, architect, Berlin, Ministry of Propaganda.

w) SCHUBERT, 1st Lt. Berlin, adjutant of the General der Flieger KESSLER who was to be the successor of GRONAU at Tokyo.

x..........

x) Dr. SCHAEFER, Berlin, Ministry of Propaganda.

15. Miscellaneous:

a) Professor Dr. HAMMITSCH and Dr. BEUEL, left during 1943 on submarine for Tokyo as interpreters for the military attache.

b). Dr. Joern LEO, Itzehoe, formerly employed in the Japanese ministry for railways, recently in Amt VI.

c) Frau Dr. WEINERT, Berlin, in Far-Eastern division of Amt VI (evaluation of information)

d) Dr. BRAUN, Legation Councillor, East Asia division chief of the Ministry of Foreign Affairs, now in SALZBURG.

e) Dr. JAKOB, secretary of Dr. BRAUN.

f) Dr. ADLER, Japanese expert in OKW-Chi (Secret Communications division)

16. Subject states that further information could be supplied by the German-Japanese Society (Berlin, Ahornstrasse 1 or 2) which was directed by Admiral FORSTER and whose secretary was Assessor TROEMEL.

17. Subject's father, Professor Dr. Willibald KIRFEL, (address: Bad Godesberg, Wiedemannstrasse 37) is a scholar of Oriental languages, Professor of Hindustani and Indology at the Bonn University, director of the Oriental Seminar. Has a thorough knowledge of the Indian circles in Germany and elsewhere and is a close friend of the Maharaja of BARODA.

E. GIS activities in the Far East:

18. Information on Far Eastern affairs reached Germany through the German Consulates and Embassies in Japan, Manchuria and Nanking, in particular through the police Attaches at these places. There also existed a secret intelligence net headed in SHANGHAI by a certain "BORIS" who sent information through the police attache of NANKING. He was in contact with a number of Germans in the Far East who appeared in his messages as sources under the cover names "FRITZ", "EMIL", "LUDWIG", "OTTO". Toward the end of 1944 it became clear that BORIS worked in contact with agents of the Russian Secret Service. He attempted to obtain authorization for conducting negotiations with the Russians for a compromise peace. Subject believes that by now BORIS is entirely under the control of the Russians. He has no details about his person except that BORIS was said to be chief of the Hitler-Jugend who had somehow remained behind in CHINA.

19. BORIS transmitted normal political, economic and military intelligence. Some of the more interesting items of information concerned are:-

a) Information about secret agreements between Japan and Russia concerning promise of non-intervention by Russia in spite of the denunciation of the Neutrality pact.

b) Information about Russian ships carrying arms and ammunition to Japanese-occupied China ports for use against CHIANG's armies. This

information.........

information came through on 2 different counts in the latter part of 1944. (Similar information - concerning Russian promise to supply Japan with tanks in case of a worsening of the Japanese military position, in exchange for a Japanese promise to hand over Manchuria, Korea and even the use of some Japanese Pacific ports to Russia - was given out in BERLIN by Dr. OGA, cultural Attache and member of the Japanese Information Service, and by KAWALERA. KAWALERA dismissed the denunciation of the Neutrality Pact by Russia as an insignificant gesture in view of secret agreements between Japan and Russia).

c) BORIS also reported about the progress of the negotiations between CHUNGKING and YENAN and about the friction between CHIANG KAI CHEK and Gen. STILWELL. In connection with this, KOISO gave a mission to General UGAKI to come to a compromise peace with CHUNGKING China. UGAKI infiltrated high Chinese officers of the WANG CHING WEI regime to CHUNGKING for negotiations, but the Donald NELSON mission foiled the plans of the Japanese,

d) BORIS also reported the existence of a secret association under KONOYE favoring capitulation to the Allies.

20. Information from BORIS and from other sources led to the belief at the end of 1944 that peace between Japan and Chungking China was imminent. This belief was based on the following:-

a) Rumor that Madame CHIANG KAI CHEK was going to sue for divorce. As she was considered the representative of the pro-American faction, this rumor was interpreted as the consequence of an imminent anti-American move on the part of her husband.

b) Elimination of members of the SOONG family from the Cabinet.

c) Death of WANG CHING WEI in Tokyo which made it possible to unite the NANKING and CHUNKING regimes under CHIANG. In this connection German circles had their doubts about the naturalness of WANG CHING WEI's death, in spite of his long disease.

21. Ever since the second half of 1944, the GIS was preparing for the eventuality of a betrayal by JAPAN and the possible switching over of the fronts (Russia and Japan vs the Western Powers and Germany). Consequently Amt VI prepared an informer net for the Far East which was to have three centers:

a) Cap St. Jacques.

b) Kalgan, Mongolia

c) Shanghai

Except for the selection of some personnel, this plan remained on paper.

22.........

22. In connection with the already reported document on conversation between Russian and Japanese officials in MOSCOW concerning future Russian plans (see para 31), Subject adds that it was obtained by Kommando "ROLAND", one of the special units of Amt VI.

F. G-2, 5th Army report of Subject:

23. We further reproduce without comment, the following report on Subject conducted by the G-2 Interrogation Center, 5th Army on 4 June 1945. This report is No. 118, CIT. Ref: CICF serial No 223 referred to in para 5 of our JZX-1647. The following interrogation was written by Capt. KOLISCH of 5th Army.

24. KIRFEL, Harald Dr. (Diplomat). Date and place of birth: 1914, SIEGBORG, Rhineland. Home address: SIEGBORG, Kaiserstrasse 51. Civilian occupation: Law student, German Foreign Office Liaison Officer (Administration) at GASTEIN. Party affiliation: SA since 1932. He joined the party in 1934. Does not remember his number. GIS career: In March 1940 Subject joined ABWEHR AMT III, BERLIN. Owing to his excellent knowledge of Chinese and Japanese he was assigned to the Far Eastern Section of the AUSLANDSBRIEFPRUEFUNGSSTELLE. This was a subsection of the Censorship Department of AMT III, responsible for collating, evaluating and editing information obtained from censorship. Subject's CO was Maj. Dr. THURNAU who was later promoted to Lt. Col. and placed in charge of the censorship Department of AMT III. Subject handled all important censorship extracts from letters written by Far Eastern nationals from all over the world. These letters were channelized through the Far Eastern Section of the Censorship Department in BERLIN which passed on the relevant material to Subject.

25. In September 1940 Subject was transferred to the interpreter school in BERLIN and, after passing examinations in Japanese and Chinese, was made instructor in these languages with officer status. During this period he prepared a comprehensive Manual on the Japanese Armed Forces (including the Japanese Intelligence Services) for the use of students at the interpreter school and for German officers who were attached to the German Military Attache's Staff in Japan. The latter were also trained by Subject. Information in this Manual were obtained partly through German Secret Intelligence sources in Japan and partly from Subject's own numerous contacts with Japanese officials in BERLIN.

26. In October 1940 Subject was transferred to the Far Eastern Section of the Academy of International Social Science. Professor HOEHN was in charge of this section. His deputy was Dr. SATO, councillor to the Japanese Embassy in BERLIN. During this period, Subject contacts Maj. WEIHRAUCH of AMT VI of the RSHA and sold him the idea of setting up an anti-Japanese Offensive and Defensive Section which would come directly under AMT VI. The work of this section would have been:- (1) To obtain all possible information on the activities of Japanese nationals in GERMANY and the occupied territories; (2) to obtain political intelligence on JAPAN through contacts with Japanese diplomatic and other official representatives, and through agents in GERMANY especially selected for this kind of work; (3) to recruit and organize a network of agents and informers who would subsequently be sent to operate with radio communications in INDO-CHINA, CHINA, YUNAN and THAILAND. The department was created as a result of objective appreciation of JAPAN's long term cynical policy which aimed at complete exploitation of GERMANY, so long as this was possible, for her own immediate war aims. Subject states that as of the end of 1943 all plans made by JAPAN were based on the assumption of a German collapse.

27 ....

27. Subject continued to work at the Academy of International Social Science (Far Eastern Section) as a cover for his intelligence work and also because it provided him with useful contacts.

28. In October 1944 Subject was appointed by the German Foreign Office to be administrative Liaison Officer to foreign diplomatics (in particular representatives to Far Eastern countries) who had been evacuated to GASTEIN in AUSTRIA from BERLIN. At GASTEIN he continued his intelligence duties reported to AMT VI in BERLIN by courier. He accompanied two Japanese diplomats to MILANO immediately prior to the German collapse and surrendered there to the Allies.

29. Subject worked in collaboration with Dr. KLASSEN, Professor at HEIDELBERG University, a Japanese scholar, who had spent a great deal of time in the Far East. Working under the Subject's direction were the following volunteers (VAU-LEUTE) and paid agents:-

VAU-LEUTE

a) TRANF ANTRON	Indo-Chinese with contacts in the Japanese Embassy. They were to have formed part of a special espionage network in JAPAN which was being organized by the Subject for service in the Far East; all of them were anti-Japanese. They should still be in BERLIN.
b) VAN MUC	
c) VAN WANG	
d) LEO, Dr.	A German with considerable Japanese experience.
e) HERZFELD, Frau Dr.	Both had considerable social contacts with Japanese and other Far Eastern circles in BERLIN.
f) WEINERT	

PAID AGENTS

g) MAYOR, Miss Alla.	White Russian, worked in the Manchurian Embassy, mother was murdered in the Russian Revolution, her father escaped to JAPAN, but was handed back to the Russians by the Japanese. She may still be in BERLIN.
h) TOTSKY, Ilona	Estonian girl who had contacts in the Japanese Embassy.
i) German girl	Subject cannot remember her name. She was Chief Secretary to the Japanese Attache.

30. All the above agents had their own network of informers, details of which are unknown to Subject. Besides these, there were also some unwitting Japanese sources classified as "I-LEUTE" by Subject. Subject's section also carried out special operations on the Japanese diplomatic premises which consisted of removing, photographing and then replacing documents of military and political interest. Such operations, which of course effected a great deal of information, details of which Subject is prepared to give, were obtained through friendly "inside contacts".

31. Subject spoke of a document removed (he does not know how) from a Japanese official, and passed on to him by AMT VI. It described a meeting of JAPANESE and RUSSIAN officials in MOSCOW in January 1945 at which the Russians clarified their foreign police in respect to JAPAN and the Western POWERS. They stated that their immediate aim was to occupy as much of GERMANY as possible, including, in particular,

the..........

the industrial areas of MAGDEBURG, DESSAU, KASSEL and all the RUHR province. They would then exploit German technical experience to build up the present deficiencies in their own armed forces, particular precision instruments, instruments for use in their Air Force, etc. Only then would RUSSIA be in a position to declare war on the Western Democracies and assist JAPAN in the Far East. This document was, according to Subject, dated February 1945.

32. Subject stated that HAMBIER, GHANDI BOSE's FREE INDIA representative in GERMANY has informed him that he had been ordered by BOSE shortly prior to the collapse of GERMANY to instruct FREE INDIA soldiers fighting for Germany to surrender to RUSSIA and not to the Western Allies. HAMBIER added that arrangements had already been made for himself to surrender to the RUSSIANS as a result of secret agreement between JAPAN and RUSSIA.

Comments and Recommendations:

33. It would seem that some form of Anti-Japanese Section of the RSHA did actually exist. It is difficult, however, at this stage to gauge how far Subject has exaggerated the scope of his own activities in order to give himself a "build-up". The possibility that the relations have been invented on the basis of directives issued him prior to the collapse of GERMANY cannot be overlooked. The presentation of the facts certainly is in keeping with Nazi Propaganda Technic.

mp

Distribution:

cc: Col. Earle B. NICHOLS	(1)
WASHINGTON	(6)
LONDON	(6)
SCI/Z/Milan	(1)
SCI/Z/Genoa	(1)
SCI/Z/Turin	(1)
SCI Unit/A	(1)
CG file	(1)
Files	(5)

Copy to H.C.S.G.
25/9.

(11

SECOND INTERROGATION OF REG. RAT HERMANN SCHERSCHMIDT
OF PERS. Z S AUSWÄRTIGES AMT,
ON TURKISH AND BULGARIAN SYSTEMS.

Attached is a report on an interrogation carried out by Major BUNDY at the U.S. 7th Army Interrogation Centre, on 29 August 1945, covering Turkish and Bulgarian Systems solved by Pers. Z S.

See Ticom/I-63 for previous report.

TICOM

19 Sept. 1945

No. of pages 4

DISTRIBUTION

British

D.D.3
H.C.G.
D.D. (N.S.)
D.D. (M.W.)
D.D. (A.S.)
C.C.R. (2)
Lt. Col. Leathem
Cdr. Tandy
Major Morgan

U.S.

Op-20-G (2) (via Lt. Cdr. Manson)
G-2 (via Lt. Col. Hilles)
A.S.A. (3) (via Major Seaman)
Director, S.I.D. USFET
(via Lt. Col. Johnson)
Col. Lewis Posell, USSTAF

TICOM

Chairman
S.A.C. (2)
Cdr. Bacon
Lt. Col. Johnson
Major Seaman
Lt. Cdr. Manson
Capt. Cowan
Lt. Fehl
Ticom Files (4)

Additional.

Lt. Col. Thompson.

This is a copy
The original has
been retained under
section 3(4) of the
Public Records Act
1958.

Introductory:

It had been requested that SCHERSCHMIDT should do a complete written paper on his work on Turkish and Bulgarian systems. As his eyes, after a recent operation, do not yet permit reading, the subjects were covered by interrogation instead. His memory is sketchy on many points, but it seems unlikely that a written account based on further recollection would add much substance to this account.

1. Turkish systems

a) Diplomatic.

The Auswärtiges Amt did not work on Turkish at all until 1934. S. believes that there was in fact very little Turkish traffic until after the MONTREUX Conference in that year. He had worked on Turkish in 1920 and believes that the codes remained basically the same (alphabetic, with Arabic lettering) until 1934.

1934 - early 1935. The main system in this period was a set of 3 4-digit codes used in monthly rotation. The codes were alphabetic within any one initial letter, but the order of the letters was scrambled. The codes were rarely used without encipherment by a

section, while SCHERSCHMIDT himself concentrated on book-building and translation, occasionally checking the work of the girls in case of difficulty. Book-building and translation were fairly difficult, because of the use of the Arabic lettering and because SCHERSCHMIDT himself was only learning Turkish as he went along.

The auxiliary system, used for less important traffic, had a single code, completely unalphabetic. Though theoretically more difficult, the code was used about half the time without encipherment and was built up accordingly, aided by one or two isolated cases of reencodement from the main system. The encipherment system, when used, was the same as for the main system and was solved in the same manner.

The two systems covered all the main diplomatic links. S. believed that there were other codes used for isolated links, as RIO DE JANEIRO and BUENOS AIRES, but there had never been enough material for a solution of these.

1935 - 1939. In 1935 the Turks switched abruptly to the latin system of literation and issued a new main system consisting of 3 codes used in monthly rotation as before. The old set of three Arabic-lettered codes was made fully alphabetic and was used as an auxiliary system for consular traffic.

the same solution technique was used as before. The code was at

The basic set of latin codes remained in use until 1939, when S. left the section. The codes were scrambled by sections in 1938; but the thread was quickly regained.

1939 - 1944 S.'s knowledge of the period is vague as he handed the section over to BENZING in 1939. When he wished to return to Turkish in 1943 there was difficulty (though not with BENZING himself) over his status, and he left Pers Z S entirely for a year. S. finally resumed Turkish in 1944, being almost entirely occupied in translation in the last months of the war.

He believes the basic codes became entirely alphabetic in 1939. They were always enciphered, but he does not know the exact system, nor the exact details of solution methods. It is assumed that the basic technique remained the same, and that the stripping was done by the less skilled personnel, while BENZING and one or two others did the harder jobs of book-building and translation. Almost complete success continued.

In addition to the main system S. recalls an unalphabetic Latin-literation code used from SWITZERLAND; this he believes to be an older code which had been compromised. Still another code was used from AFGHANISTAN and beginning in 1944 from GREECE. At first this was not enciphered and the book was built up to enable solution of later enciphered AFGHANISTAN traffic.

This is a copy
The original has
been retained under
section 3(4) of the
Public Records Act

2. Turkish systems

b) Military.

While the Auswärtiges Amt did not handle military traffic habitually, the Turkish military traffic was made available to them, and they tackled it when time permitted.

The first solutions were achieved in 1936-7 and continued until 1939, although there was very little traffic in this period. The code was 5 Z, and was sometimes enciphered by a primitive method taking only one or two digits of each group and leaving the rest unchanged. Solution was aided by a common "General Staff" address which came to four groups in the new Latin literation, and by one case of a direct reencodement from a message sent in the diplomatic code.

After 1939 a new code was introduced, and S. is unable to give any details of BENZING's work on it. He has the impression that spasmodic success was achieved, but the bulk of the work on this was done by OKW. (The OKW section was headed by REG. RAT Dr. LOCKER, and had more people than PERS. Z S. S. had a low opinion of the linguistic ability of the OKW translators, and did not think the results were in proportion to the numerical difference. He believes OKW had considerable success with Turkish military systems.)

3. Bulgarian Systems. S. stressed that this was not his main job and was done largely on a spare-time basis. Before 1938 Bulgarian work was not considered important at all, and only a few

scattered efforts were made. S. went to work on it in earnest only in the Summer of 1941.

The main system consisted of two basic codes, used on the same links for material of different security importance. The codes were 5 Z, with about 20- 30,000 actual values before 1939, and 30- 40,000 thereafter. The basic code was changed once between 1939 and 1944, S. thinks in 1941, and the former top security code then became the auxiliary system.

Except for one 2-3 month period the codes were not enciphered. Up to 20 links were served by providing a different pagination for the code twice a month on a single link. Within the pages the values were written in a cyclic alphabetical order, but the cycle might start in the middle of a page and run backwards or down and then up, or in a variety of ways.

Solution depended entirely on the amount of traffic. Any major link could be solved at will if the effort could be made, and in fact from 1943 on all major links were read. The basic code had been completely recovered by that time and the pagination could be built up correctly, with the aid of "Reference", numbers, special names, and lettered values which gave very common groups. The chief difficulty was to break the additional special pages provided for the use of each link, with personal and geographical names. As a whole solution was never a difficult technical operation.

S. knows nothing of Bulgarian military systems.

TOP SECRET

D/13(1)/1464

Mr. F.A. Kendrick

With reference to the attached documents, I would be grateful if Thornett, or anyone else concerned, could provide me with a questionnaire for KIRFEL.

Major Seaman has suggested the following questions :-

(1) What other Japanese crypto materials were lifted ?

(2) What success did German cryptanalysts have with Jap systems ?

(3) Describe fully the Japanese machine mentioned para 10. Could Germans read the machine messages ?

Would you please return the enclosures in due course with your reply.

[illegible] September, 1945.

Kendrick

for Bonnett

[illegible] following questions [illegible]

What other [illegible]

[illegible]

What [illegible]

[illegible]

[illegible]

[illegible] the

[illegible]

[illegible] the

[illegible]

Cdr. Dudley Smith
S.A.C.

B(2)

Cx 12799/1862 returned herewith.
There is no immediate prospect of this being issued in the I series owing to pressure of work so I thought you would like to have it back in order to reply to Para 2 of DF7's minute.

As regards publication in the I series do you think Paras 6 – 17 inclusive would suffice?

A. Cowan
for TICOM D.D.

3/9/45. [illegible] would not like to publish [illegible] report because SSA [illegible] Interrogation [illegible] [illegible] [illegible] [illegible] [illegible] permanently a Company [illegible]. OK? [illegible]

Hom D.O.

Forwarded. I think this report (or extracts) should be issued in the I. Series.

I will have to reply to the second para of V F7's minute of 30.8.45.

Dudley Smith
S.T.C. 2.9.45.

PUBLIC RECORD OFFICE

Group/Class HW 40

Piece 181

TICOM/I-89 retained under S3(4) of the PRA 1958

(date) 11/2/2004

(Signed)

⑧

[illegible]

[illegible]

7th September, 1942.

Dear Bull,

Herewith the brief for Fraulein [illegible], as promised, together with spare copies of [illegible], J-47 and J-46.

I have rather spread myself on some of the items in the questionnaire, but think it better to put in too much rather than too little. Doubtless she will be unable to answer a lot of them.

In dealing with Section I ([illegible]) you should affect an attitude of bored indifference. Don't give her the impression we're particularly interested and don't press her if she doesn't respond.

Bon voyage.

Yours sincerely,

Commander O. Bull, R.N.V.R.,
[illegible] Branch.

(Copies to :- [illegible]
[illegible]

PUBLIC RECORD OFFICE

Group/Class HW 40

Piece 181

Questionnaire attached to minute dated 7 Sept 1945 retained under S3(4) of the PRA 1958

(date) 11/2/2004

(Signed)

PUBLIC RECORD OFFICE

Group/Class HW 40

Piece 181

Minute dated 2 Sept 1945 retained under S3(4) of the PRA 1958

(date) 11/2/2004

(Signed)

copy to D.D.(CSA)

TOP SECRET

TICOM/D-16

Attached are translations made by SSA of Annual Progress Reports by Pers. Z.S. covering 1927, 1941 and 1942 and bearing the following titles:-

1. Progress Report of the Group England and the Spanish and Portuguese speaking countries. Aug. 8, 1927.
2. Annual Report for 1941 on the Group British Empire, Thailand, Portugal, Spain, Latin-America.
3. Cryptographic Work in the Group Great Britain, Siam, Portugal, Spain and Latin America - Hagen 1-2-43
4. Annual Report for 1942 on the Section British Empire, Ireland, Thailand, Portugal, Spain, Latin America.

TICOM
28 August 1945

No. of Pages 20

Distribution

British
Director
D.D.3
D.D.4
D.D.(N.S.)
D.D.(M.W.)
D.D.(A.S.)
D.D.(C.S.A.) (2)

U.S.
OP 20-G (2) (via Lt. Pendergrass)
G-2 (via Lt.Col. Hilles)
S.S.A. (2) (via Major Seaman)
Director S.I.D. USFET
(via Lt. Col. Johnson)

TICOM
Chairman
S.A.C.
Cdr. Bacon
Cdr. Mackenzie
Cdr. Tandy
Lt. Col. Johnson
Lt. Col. Lewis Powell
Lt. Cdr. Manson
Major Seaman
Major Morgan
Capt. King
Capt. Cowan
Lt. Vance
Ticom Files (2)

Additional
S.A.C. for D.D.(C.S.A.)

[illegible]

Progress Report
of the Group Dealing with the Spanish and Portuguese Speaking Countries

August 8, 1947

[illegible] in this group during the last year [illegible] by [illegible] the messages which could then be [illegible] those which could not be solved. [illegible] could be read [illegible] Portuguese [illegible] all other countries [illegible] a real change [illegible] the period concerned [illegible] current [illegible] solved [illegible] on the solution of the [illegible] developed [illegible] another [illegible] Portuguese speaking [illegible] Due to [illegible] more [illegible].

[illegible] September of 1947 [illegible] preliminary work was [illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

04 225 253 261 301 311

On the basis of incoming telegrams these could be further perfected and in part corrected so that now all incoming telegrams are read almost in their entirety.

Spanish codes have developed only very slowly as completely alphabetic codes. The size of the new as well as of the old code is always 10,000 groups. The oldest which are still in use are still being transposed alphabetically within the individual pages and the page numbers are transposed. In the case of the more recent codes the page numbers and the line numbers are transposed. The vocabulary of the individual pages always remains the same. Once we succeeded in determining the page numbers of a new code there were only 100 possible meanings for each group. The meaning of the individual group is therefore much easier to determine. In all Spanish codes the last two places of each group are read first. In June, 1927, a telegram was noticed in code "00" which was relayed some days later to another office in a slightly changed form in code "04". In this way it was possible to determine some 50 groups. Since then we have succeeded in determining almost all the page numbers of the code. The content of the telegrams consists chiefly of reports on shipments of weapons and on suspicious persons. Further intensive work will be required for the development of the code.

Argentina

Only one code is used for Argentine telegrams. The code is arranged alphabetically and the major part of the vocabulary is in the general section, at the close are the following special sections: spelling table, dates, numbers, year dates, list of names, list of nations and cities as well as a list of Argentine diplomats. In spite of the systematic alphabetical structure of the code, a complete solution of the telegrams calls for a great deal of effort since the code is extremely comprehensive and offers many compound forms. The main vocabulary of the code comprises 65,500 groups to which are added the above named lists so that the total extent of the code runs over 101,000 groups. Work was begun in 1927 and the code is now so far solved that incoming telegrams can be read roughly, although not always completely.

Beginning the first of January in 1926 the number 100 was added to each 5-place group and must be subtracted before decoding.

In the traffic of the Argentine Government with the naval mission in Italy and with other naval attaches a cipher system is in use which has not yet been worked on.

Chile

Work on the Chilean telegrams which we have been able to solve since March, 1924, was started in August, 1926, and could be completed successfully within a short time. It developed that the previously used and already solved systematic 5-letter code with 26,500 groups was still being used. Only the first and last two letters of each group were being transformed with the aid of a digraphic substitution table. The table was quickly solved and the telegrams read once more.

Ecuador

Since the end of 1923 an exchange of telegrams between the Government of Ecuador and its representative in Berlin has been observed. The telegrams consist of non-pronounceable 10-letter groups. In the autumn of 1926 we began work on this traffic and it appeared that the division of the cipher text into 10-letter groups was purely arbitrary. For encipherment a code is used consisting of 2, 3 and 4-letter groups which, after conversion, are run together and transmitted in groups of 10 letters. The division of the groups is recognized by the vowels since the first letter of every group is a vowel, while the other letters of the group are consonants. The code is not in strict alphabetical order; solution has progressed to a point where all incoming telegrams can be read entirely.

Mexico

Telegraphic traffic of the Mexican Government with its representatives abroad is entirely with the aid of cipher systems; no code is employed. When work was begun in the autumn of 1926 it came out that Mexico in the previous years used the same key for rather long periods. Not until 1926 did they begin to improve their cipher system by combining 5 alphabets of a 26-alphabet table to form a key which would be used for several days, and finally in 1927 they began to use a separate key for each telegram. The system itself consists of a 5-place Caesar, i.e., the text to be enciphered is divided into groups of 5 letters and then the first to the fifth letter of each individual group is enciphered by a particular substitution alphabet. For transmission two groups are combined, hence, incoming telegrams consist of 10-letter groups. As mentioned above, most of the back keys and nearly all the current keys have been solved.

Colombia

Colombian traffic is enciphered very much like the Mexican with the aid of 5 successive substitution alphabets. Telegrams on hand have been solved and since the tables are always used for several telegrams, solution of this traffic ought not to cause any particular difficulties in the future.

Bolivia

Like Mexico and Colombia, Bolivia for its telegraphic traffic uses a cipher system. While the two previously mentioned countries use 5 alphabets, Bolivia uses 10 in sequences. Even though the longer telegrams could be solved, the difficulty involved with this system is so great that single telegrams, particularly short ones, cannot be read

Peru

In regard to cryptographic technique, Peru is the most advanced country of all those in Central and South America. In telegraphic traffic a 5-letter code with pronounceable groups is used which contains 10,000 to 20,000 values. Due to the extremely scanty material, 45 telegrams in 7 years, any attempt to break the system appears futile. If, in the future, more material should come in, this code should be soluble without too great difficulty, thanks to the great help afforded by the transmission of proper names by spelling system.

Uruguay

The telegraphic traffic of Uruguay is likewise so slight that no work is being done at present. Without further investigation we can say that, with more material, success could be attained without too great effort since it is merely a 2-digit encipherment employed with a short code.

Portugal

The Portuguese Government uses for telegraphic communication with its representatives 5-digit codes of 60,000 to 70,000 groups. In the autumn of 1926 we began working on Portuguese material. As formerly, so today, with Portuguese codes, the last three digits of the 5-digit code group are to be read first. It was ascertained that for each circuit a particular code existed. For the Berlin-Lisbon, Lisbon-Berlin traffic, which was attacked first, it could be shown that this code can be reduced by means of a 1000-place substitution table to a code in use earlier. The 3 last digits of the 5-digit code group, which are to be read first, correspond to the page numbers of the code which have been changed in respect to earlier codes, while the line numbers continue unchanged. When the work had progressed so far that we could recognize the approximate content of the telegrams, in February, 1927, a change took place in this traffic. Whether this new code can be reduced by any such measures to the known code has not yet been determined. On the other hand, in the case of the code used between Bucharest and Lisbon, this possibility has been proven and if more personnel is available a rapid solution should be possible.

Brazil

Since March, 1926, a new code has been used in Brazilian traffic. The work on this, begun in the past few weeks, shows that it is again an alphabetical code constructed very much like the one formerly in use. As before, the last 3 digits of the 5-digit group are read first. The number of groups, 94,[illegible] in the old code has been expanded by [illegible],000 in the new code, from which we conclude that the expansion of the code has taken place by introduction of new concepts. Solution is rather difficult because of the lack of material (70 messages). However, a good skeleton has been obtained for further work in the groups already solved.

Conclusion

In conclusion it is neceasary to say a few words on the personnel question. Even though in the period under report the codes and ciphers of most of the Spanish and Portuguese speaking countries have been solved, the help available is by no means adequate to develop these codes to the point where all telegrams can be read completely. It is absolutely necessary that in the present status of the work an assistant with a complete mastery of the language concerned be available for each of the two language groups. If this is not the case, then sooner or later things will bog down again and in view of the progressive difficulty of the codes and ciphers, it will not be so easy to get a fresh start once more.

Furthermore, in the future the English materials must be worked on more intensively. The two codes worked on and solved, "B10" and "B12" call for a separate assistant to make possible further development. For the new work (numbers) one permanent assistant is the least we must have.

To make possible further successful work we should therefore need:

For English codes "B10" and "B12"	1
Statistical work	1
Spanish group	1
Portuguese group	1
Total	4

Berlin, 8 August 1927
Ernst Hoffman

Annual Report for 1940
on the Group
British Empire, Holland, Portugal, Spain, Latin America

England

Worked on:

a) English Digit Systems:
The "Interdepartmental" [illegible]. The [illegible] of this system was captured and the solution of [illegible] was worked out from that to [illegible] O.K.W. on the [illegible] in [illegible].
Some telegrams from the Middle East could be read. Toward the end of the year the receipts were so slight that further work on this material no longer appeared worthwhile.

b) English letter systems:
1) "B 25", a non-systematic 4-letter code with 16,224 groups. It was solved and so far developed that telegrams could be read for a considerable period almost without gap. In the autumn of 1940 a captured original was sent us which made possible complete reading of telegrams.
2) "B 22", a systematic 5-letter code with 84,000 groups. It was solved and telegrams have been read for approximately 3 years. In the summer of 1940 we were given a captured original.
3) "B 30", a non-systematic code of 4-letter groups used in the Near, Middle and Far East. Traffic received was slight; however a beginning was made in setting up an index and the cross sum of the groups as well as the size of the code was determined.

Not worked on:
The consular system and Teneriffe-Las Palmas traffic, involving transposed plain text, in which only a few telegrams were received.

South Africa

Worked on:
a) "B 22" (see England b 2), and
b) "B 29", a systematic 5-letter code of approximately the same size as "B 22" which was solved and so far worked out that the rare incoming telegrams can be read almost without gaps.

Not worked on:
A letter system used in traffic with Stockholm, due to want of material. The last telegram of this type was received 16 December, 1940.

Ireland

Worked on:
a) "B22" (see England b 2), and
b) "B22" enciphered. This code was [illegible] with [illegible], which [illegible]. The

encipherment table is so used that one 5-place group is replaced according to $T26_{n}$, the following group by $T26_{n\ 1}$, $T26_{n\ 2}$ or $T26_{n\ 3}$ or else $T26_{n-1}$, $T26_{n-2}$ or $T26_{n-3}$. All Irish telegrams can be read completely.

In 1941 223 Irish telegrams were read.

·Canada

Worked on:
"B 22" (See England a 2)
Not worked on:
A 5-letter system in which only isolated telegrams were received.
In 1941 583 British Empire telegrams were read.

Thailand

Worked on:
A systematic 5-digit code in English language with 110,000 groups. For the last 10,000 numerical groups usually pronounceable letter groups of indefinite length are given. A part of the telegrams is enciphered, i.e., there is added to or subtracted from the line number of the groups a multiple of 5 according to an indicator. Telegrams are read almost without gaps.
In 1941 97 Thailand telegrams were read.

Portugal

Worked on:

a) A partially systematic 5-digit code with 50,000 groups. Encipherment on the different circuits is in the following fashion:
   1. By subtraction or addition to the line number of a sum fixed for the circuit concerned.
   2. By transposition of the group elements.
   3. By 1000-place substitution tables for the page numbers.

b) A partially systematic 5-digit code with 61,500 groups. It is enciphered with 20 distinct 100-place substitution tables for the line number of the groups and on some circuits also with a 1000-place table for the pages. In addition there is a letter encipherment to avoid repititions, i.e., a 100-letter table for the line number and a 1000-letter table for the page number. Moreover, for each circuit there is a distinct transposition of the group elements.
   A large part of the telegrams were read with some gaps.
   In Berlin-Lisbon traffic telegrams sent in this code were not read because keys changed so frequently and receipts were so small that only in a few cases did the work yield any practical result.

c) A partially systematic 5-digit code with 61,800 groups with encipherments of the type described in paragraph b. The numerical encipherments were solved and beginnings made in the solution of the code. Because of the slight receipts and lack of personnel for Portuguese, work was not continued.
   In 1941 66 Portuguese telegrams were read.

Brazil

Worked on:

a) Letter systems

1. "Bras. B1", a systematic 5-letter code with 165,625 groups. The telegrams were read almost without gap.
2. "Bras. B2", a partly systematic 5-letter code with 82,000 groups. After 2,200 groups had been recovered and a series of telegrams read with some gaps, a copy of the original code was placed at our disposal by O.K.W. which made possible a complete reading of all telegrams.

b) Digit systems:

1. "Bras. Z1", a systematic code with 100,000 5-digit groups. The telegrams were read almost without gap.
2. "Bras. Z7" and "Bras. Z8". Encipherment of "Bras. Z1" by means of 1000-place tables for the page numbers and interchange of group elements. The telegrams were read almost without gaps.
3. "Bras. Z3", a code with 80,000 digit groups, which was put together from "Bras. B2" by the exchange of the page numbers and displacement of row digits on a multiple of 10. Work has just begun (February 1942) on the still limited material.
4. A 5-digit probably systematic code with 100,000 groups was enciphered with a table of letters. The 300 pairs of letters occurring in the first and second or fourth and fifth places were reduced by equating to a 100-place table for the first and second and one for the fourth and fifth places and the 26 middle letters (in the third place) have likewise been reduced by equating to a 10-place table. The conversion to numbers proceeded slowly because of the very sparse incoming material. From the 23rd of December 1941 to the breaking off of relations (29th of January 1942) only one telegram of this sort was received.

In the year 1941, 248 Brazilian telegrams were edited.

Spain

Worked on:

A 4-digit, partly systematic code with 10,000 groups called "94". The telegrams enciphered in this code in the traffic Madrid-Bogota, Quito, San Salvador, Sofia, San Juan de Puerto Rico and in part Guatemala were completely read. The remaining traffic was only noted. The traffic Madrid-Berlin fell off almost entirely; in 1941 eight telegrams were received.

In the year 1941, 34 Spanish telegrams were edited.

Argentina

Worked on:

a) A 5-digit systematic code with 110,000 groups. In most of the traffic there was a change of groups through addition or su subtraction of a constant sum. Occasionally, also, in one and the same telegram addition and subtraction were used interchangeably. The traffic was solved and the telegrams were read and edited almost without gaps.

Bolivia

Worked on:
A [illegible] code with 73,000 groups is enciphered with 1000 and [illegible] code-tables for the pages and row columns and in frequently changing regrouping of the group elements. The incoming telegrams which were both very sparse and uninteresting in content could be read with some gaps.
In the year 1941 one Bolivian telegram was read.

Chile

Worked on:
A 1 to 4 letter systematic code with 42,000 groups was built up by the autumn of 1940 to such a point that the telegrams were read almost without gap. A photocopy of the captured original which was placed at our disposal at that time made possible a complete reading of the telegrams from that time on.
Not worked on:
A very sledom used systematic, 4-letter code in consular traffic (Passport) and a new diplomatic code, on account of the still limited material. Up to this time 12 telegrams have been received since the 25th of August, 1941.
In the year 1941, 273 Chilean telegrams were read.

Dominican Republic

Worked on:
Columnar system (Spaltenverfahren) with 5 T26, which is applied to the plain text. Occasionally, also, plain text passages appear in the enciphered messages - the keys were solved and the incoming telegrams were accordingly completely read. In the year 1941 one Dominican telegram was read.

Ecuador

Worked on:
A 2 to 4 letter systematic code with 61,945 groups with interspersed clear text. The code was solved and the messages could be completely read.
Not worked on:
A letter consular system, in which only one telegram was received.
In the year 1941, 25 Ecuadorian telegrams were read.

Colombia

Worked on:
Columnar systems with 5 to 15 T26, which are directly applied to the plain text without any text between. The telegrams, which came in at great intervals, were read by the solution of the current substitution table.
In 1941, 45 Colombian messages were read.

From Guatemala, Havana, Panama and Paraguay the incoming messages are so extraordinarily unimportant that not once was it worth taking note of them.
From Panama and Guatemala one plain text message was read.

In 1941 from this group a total of 1639 messages was read.

Personnel

Section Head: Miss Hagen
Colleague on English, Portuguese and in part Spanish: Miss Wernick
Colleague on Spanish: Miss Noll
Assistants: Miss Feldbaum
" v. Kaisenberg
" Kleppin
Mrs. Offermann
Miss Roebcke
" Seele
" Tirschack

Berlin: 11 November 1942

Translated by Lt. M. C. Lane

Argentina

With a systematic 5-digit code of 110,000 groups on many circuits changes in the groups are made by addition or subtraction of a constant.

Bolivia

A 5-digit code of 78,000 groups is enciphered with a 1000-place or 100-place letter table for page or line numbers and by simultaneous re-grouping of the group elements. Replacement [illegible] quite irregular.

Dominican Republic

Substitution system with 5 alphabets applied to the plain text. Replacement quite irregular.

Colombia

Substitution system with 5 alphabets applied to the plain text. Replacement quite irregular.

Mexico

According to approximately 100 indicators each group of the systematic 5-letter code is changed into a group lying 1-100 places farther on in the decoding section. No change in mode of encipherment has been made.

Peru

As encipherment for the partially systematic 5-letter code digraphic and trigraphic tables are used for the first and second and the third, fourth and 5th letters, respectively. These tables are different for each circuit. No replacement of tables has been made.

Uruguay

Plain text interposed between groups of a 4-letter code are enciphered with a 100-place numerical table, so that for each letter of plain text or for a consonant plus following vowel a 2-digit number is substituted. Frequent endings and punctuation are represented by 3-digit numbers, e.g. 333 = ion. Replacement very irregular.

Venezuela

Plain text introduced between the groups of a systematic 4-letter code is enciphered by a substitution system with one to ten alphabets. Moreover, on some circuits the groups are pushed along from 1 to 10 positions in the code. Replacement is quite irregular.

Hagen
1-2-42

ANNUAL REPORT FOR 1942
ON THE [illegible]
BRITISH EMPIRE, IRELAND
[illegible]LAND, PORTUGAL, SPAIN
LATIN AMERICA

BRITISH EMPIRE

[illegible]

[illegible]

[illegible] Systems

1. [illegible] place systematic code
2. [illegible] non-systematic code
3. [illegible] non-systematic [illegible] the same fashion as [illegible], but with [illegible] was made in the [illegible] procedure [illegible] simple substitution alphabet of 26 [illegible]. [illegible] was begun after the [illegible] in the spring of 1942 but was again laid aside [illegible] because other work was more pressing. [illegible] was taken up again and by the end of [illegible] had been broken. On the first of [illegible] telegram was read. The incoming [illegible] and the outgoing [illegible] read currently.
4. [illegible] non-systematic letter [illegible] constructed in almost the same fashion as [illegible] in use since 1 May, 1942. [illegible] in May and [illegible] work in June. [illegible] had been recovered. [illegible] in October, 1942. [illegible]

[illegible] Codes:

[illegible] in the summer of 1942.

[illegible] 1942 [illegible] January 1943.

[illegible] worked on:

a) English numerical systems (excep. TPC)
b) [illegible] system used between Teneriffe and Las Palmas in which [illegible] of the [illegible] was a code of transposed plain text. [illegible] informed us in February, 1942, [illegible] attempts at solution were made then.
c) The "Indian Code" (original designation), a systematic 5-letter code which was laid aside due to lack of material after a start at solution had been achieved.
d) An unsystematic 4-letter code of approximately 1,000 groups [illegible] worked on due to lack of adequate material.

[illegible]

[illegible] was done on:

[illegible] (see England a 2)

[illegible]

[illegible] on:
[illegible] (see England a 2)

[illegible]

[illegible] on:
a) [illegible] (see England a 2)
b) [illegible] systematic 5-letter code.
[illegible] worked on:
[illegible] system used in traffic with Stockholm [illegible]
[illegible] only [illegible] messages were received.
[illegible]

[illegible]

[illegible] about the end of August [illegible] and beginning of November [illegible] 16th of December [illegible] exchange of [illegible] at the request of [illegible] contact with [illegible] exchange of ideas. The [illegible]

[illegible]

[illegible] on:
a) [illegible] (see England a [illegible])
b) [illegible]

Not worked on:
A further system due to inadequate material.
In 1942, 126 Irish telegrams were read.

Thailand

Worked on:
A 5-digit code in English language with and without encipherment. On the [illegible] of October, 22nd of September and 31st of December, 1942, there were changes of keys on the Berlin circuit. In place of the previously used addition or subtraction of a multiple of 541 to the [illegible] number of the group, a 5-place additive sequence is being used. [illegible] and words not contained in the code are enciphered by a substitution table. Moreover, irregular spelling groups beginning with [illegible] used for geographical names have been replaced by others [illegible] with J.
In 1942, 139 Thailand telegrams were read.

Exchange with F.A.

At the beginning of 1942 the Thailand code was turned over to F.A. for copying.

Portugal

Worked on:
a) [illegible] *, a 5-digit, partially systematic code of 50,000 groups with encipherment. In the autumn of 1942 a new 1000-place substitution table used for this code on the [illegible] circuit was solved so that the home telegrams, which in the summer of this year were mostly sent in '[illegible]' (see [illegible]) and thereafter almost exclusively in '[illegible]', could be read again.
b) [illegible] *, a partially systematic 5-digit code of [illegible] groups with encipherment.
c) [illegible] *, a partially systematic 5-digit code with [illegible] groups with encipherment.
d) [illegible] traffic between Lisbon and Luanda in which [illegible] of-letter substitution is employed for enciphering [illegible] plain text.
Not worked on, [illegible] due to inadequate material:
a) [illegible]
b) [illegible]
c) traffic [illegible] colonies with [illegible]
In the course of the year 1942, [illegible] Portuguese telegrams were read.

[illegible]

On 11th [illegible] [illegible]

[illegible]

Brazil

Worked on:

a) Letter systems:

1) [illegible] B1), a systematic 5-letter code with 100,000 (possible) groups.

2) [illegible] B2), a partially systematic 5-letter code with [illegible] groups.

b) [illegible] systems:

3) [illegible], a systematic code with 100,000 groups which is yet [illegible] used in isolated cases between [illegible] and Rio.

4) [illegible], which is derived from [illegible] type numbers and substitution of page numbers. Since [illegible] in very [illegible] - in the [illegible] eight [illegible] telegrams - no telegrams could be read in spite of good [illegible] in the work.

In 1942, 130 Brazilian telegrams were read.

[illegible]

Worked on:

[illegible] (so-called for the indicator group of [illegible]), [illegible], partially systematic code with 10,000 groups.

Not worked on:

[illegible] other systems. Berlin traffic is very [illegible] and [illegible] would have to be watched and in time [illegible]. No attempt was made by [illegible] or by [illegible]. [illegible] that machines were employed.

[illegible] 1942, [illegible] Spanish telegrams were read.

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible] on:
[illegible] received, systematic letter code for consular traffic
[illegible]).
[illegible] only sporadically until mid-November, 1940.
[illegible] December, 1942 [illegible] was introduced [illegible]
[illegible] available [illegible]. The [illegible] themselves [illegible]
[illegible] system, [illegible] few messages [illegible] in
[illegible] read. The [illegible] apparently is not
[illegible]
[illegible]

[illegible]

[illegible] on:
[illegible] code.
[illegible] on:
[illegible] in letters in which only [illegible] telegrams [illegible]
[illegible]
[illegible] telegrams were read.

[illegible]

[illegible]
[illegible] 5 to 15 [illegible] (substitution [illegible])
[illegible] (see [illegible]
[illegible]).
[illegible] telegrams were read.

[illegible]

[illegible]
[illegible] systematic 5-letter code [illegible].
[illegible] 5-letter code were [illegible]
[illegible]
[illegible] of the [illegible]
[illegible] of this kind could be read. [illegible]
[illegible] the original [illegible]
[illegible] November, 1944, [illegible]
[illegible]
[illegible] 1944. Since then the few [illegible]
[illegible]
[illegible]
[illegible]

[illegible]

[illegible]

[illegible] 1942, [illegible]
[illegible]

[illegible] group.

[illegible]

The development of a partly solved, partially [illegible] [illegible] has been postponed temporarily due to lack of personnel. This will be resumed in the near future.

[illegible]

[illegible]
[illegible] 4-letter code with 100 place substitution table [illegible]
[illegible] used.
[illegible] different alphabets were used.

[illegible]

[illegible] 4-letter code with encipherment.
[illegible] with 5 or 10 [illegible]
[illegible] 15 [illegible] different alphabets were used.

[illegible]

[illegible] to the end of 19[illegible] [illegible]

[illegible]

[illegible] of relations [illegible]

[illegible]

[illegible]

[illegible] Dr. [illegible]
[illegible]
[illegible]

[illegible]
[illegible]

[illegible]

[illegible]

4

TOP SECRET

[illegible]/1484.

D.D.(C.S.S.)

(Copy to :- D.D.A.)

Examination of some of the documents listed in [illegible] of 14th July, 1945, in conjunction with the [illegible] Annual Reports for 1941 and 1942 ([illegible]/1262 of 14th June and 1327 of 15th July) gives the following identifications of the [illegible] "B" classifications of British civil systems :-

(i) Certain

B.16. Foreign Office [illegible] Code ([illegible]).

B.[illegible]. Government Telegraph Code ([illegible]).

B.[illegible]. Foreign Office [illegible] Code ([illegible]).

B.30. India Office Confidential Code [illegible] ([illegible]).

B.31. Foreign Office [illegible] Code ([illegible]).

(ii) Probable

B.23)
B.24.) South African version of [illegible].
B.25.)

10

[illegible] August, 1945.

PUBLIC RECORD OFFICE

Group/Class HW 40

Piece 181

TICOM/D-3 (cont?): retained under Section 3(4) of the Public Records Act 1958

(date) 11/2/2002

(Signed)

✓ Pers ZS Records (abstracts)

②

(16) B.26. Südafrika

BEHUN
BYZFI
DYWXI
LOWMO
MYTKE
NAKIK
TYROW
VOZRO

✓ (9) B.17.

A-b = 1
d = 2
e-f = 3
g = 4
i-k = 5
l = 6
m 7
n 8
o-p 9
r 10
s 11
t 12

12n + 1 = 13, 25, 37, 48, 61
73, 85 usw.

AMGOL
BIDRO
DISEG
EPFAP *
FEKOM *
KASSU *

RAPTI

Sent to KA

(13) B.23

ABAIB	A
ABAOD	A
AJHWI	all
ALUDI	and
DALYI	comma
GUJWH	⊙

(48) B.26. Prunus Capetown
Oppenkelly London } v Defence Pretoria
Saley Berlin

(47) B.27 Prunus Capetown v Saley Berlin 4/39
? 4 letter Book

SGHP
TIYS
OYXV
IZZA

30/8/38 Saley Berlin v Prunsec.

~~(? Recorded.)~~

(14) B.24

ANCB~~E~~U	and
OVEVG	
UXTVL	stop
YM~~E~~YUW	

(17) B.30

IV

(B.25 deleted).

? unused old book.

ODỤD	⊙
KZAH	⊙
WAVU	⊙–┘‾

(i.e. "Q")

AAIG	necessarily
MI	1939
PD	Sentenced, sentiments
QG	(? starts up)
VM	wise wisdom
YB	have not yet, been
ABAA	Minister of War Production
BH	demanded.

etc.

(10) Band 1 B.18

(11) 2

(2 copies)

KYSU	⊙
ƵSIZE	⊙
TECA	⊙

(i.e R.1930)

AABY	then
CF	lead, letter follows
FH	as the
GO	Li-Tsung-jen, liberate
HU	~~Liberate~~ and that
IX	WU
ME	personality, of persona grata

etc.

(54) B.20 Prodrome London
Bucharest

Preamble in R. 1930 (TECA)

JEBY (1932)
UDUC
FUOC
SUUN
OXYX

㊽ 3.17 RAPTI (RIPTA) Prodrome
Berlin
SASUK (KASSU)
OBTED Preamble
in R.1930

1930 – 32

⑮ B25 ALLA ⊙ i.e. R.1935
FAKE ⊙
NOAH ⊙

}
ASAD defence
BK seems
CR at most
DF sea

etc.

(56) B.31 Prodrome Ln v Naples 14.3.45
(SISR)
i.e. R.1941 NWEES PHIZK VVFQC
VQRJX VQRTW ZIONN etc.

(55) B.22 GTC Traffic

A HOOA
ABLIV
AZFIV
ABABY

B. 18 ✓ R. 1920 ?

19

20 { [illegible] F.O. [illegible] (JEBY)

21 ?

✓ 22 ✓ GTC 1922

23 [illegible] (ALUDT)

24 [illegible] (ANCBU)

✓ 25 ✓ R. 1935

26 [illegible] (BEHUN)

27 ~~[illegible]~~ [illegible] 4 [illegible] (TIYS 122A)

28 ?

29 ? I.W.C.

30 ✓ Q. 1935

31 ✓ R. 1941

C.C. [illegible]

D.O. [illegible]

D.C. [illegible]

(18 [illegible]
[illegible])

22.2/1327 [illegible]
[illegible]

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
7		[illegible] 5. [illegible]		(43) 1931/32	F.O. (KASSU)
8	✓ [illegible]	4. [illegible] [illegible] 40% [illegible]	10/35 30/3/35		
[illegible]					
[illegible]		4. [illegible]		(E4) 1933/34	F.O. (JEBY)
21					
22	✓ G.T.C. 1933	5. [illegible] [illegible]	[illegible] 4 2/43	(55) 3/45	[illegible] FILE [illegible]
23		[illegible] (13) [illegible]			ALUDT
24		5. [illegible] (3) [illegible]			ANCBÚ

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
B.25	✓ [illegible]	2 [illegible] United Kingdom (13) [illegible]	On [illegible] [illegible] 2/43		
B.26		5 [illegible] South Africa (16) Fees statistics		(146) 1938/39	(BEHUN)
B.27		4 [illegible] [illegible] South Africa 4 letters bad		(147) [illegible]/39	(TIYS.122A)
B.28					
B.29	IWC				
B.30	✓ [illegible]	4 [illegible] United [illegible] (17) [illegible]	[illegible]		[illegible]
B.31	✓ [illegible]	4 [illegible] United Kingdom	E.I.F. I.E.H.C.	[illegible]	[illegible] See [illegible]
[illegible]	[illegible]	5 [illegible] Africa			

(B) Copy to D.D(CSA)
12/8.

15(Q)

1

TOP SECRET

Polish
Turkish

TICOM/I-63

INTERROGATION REPORT ON
ORR HERMANN SCHERSCHMIDT
OF PERS. Z. S., AUSWAERTIGES AMT

The attached document is a report on the interrogation of ORR Hermann SCHERSCHMIDT of Pers. Z.S., Auswaertiges Amt, by Major W.P. Bundy, AUS and Capt. J.K. Lively, AUS at HEIDELBERG on 1st August 1945. SCHERSCHMIDT is a specialist in Turkish and Slavonic code-breaking.

TICOM
11 August 1945

No. of Pages 4

DISTRIBUTION

British
Director
D.D.3 (2)
D.D.4
D.D.(N.S.)
D.D.(M.W.)
D.D.(A.S.)
A.D.(C.C.R.)(2)
Lt. Col. Leathem

U.S.
OP 20-G (2)(via Lt. Pendergrass)
G-2 (via Lt.Col.Hilles)
S.S.A. (2)(via Major Seaman)
Director, S.I.D. USFET
(via Lt. Col. Johnson)

TICOM
Chairman
S.A.C. (2)
Cdr. Bacon
Cdr. McKenzie
Cdr. Tandy
Lt. Col. Johnson
Lt. Col. Lewis Powell
Lt. Cdr. Manson
Major Seaman
Lt. Eachus
Lt. Vance
Capt. Cowan
Lt. Fehl
Ticom Files (2)

Additional
Major Morgan

Interrogation Report on Oberregierungsrat

HERMANN SCHERSCHMIDT

Of Pers. Z.S., Auswaertiges Amt

At Heidelberg
1 August 1945

Interrogators:
Major W.P. Bundy, Sig. C.
Captain J.K.Lively, Sig. C.

1. Circumstances. Scherschmidt was located in the eye clinic of the Heidelberg University Hospital, recovering from a cataract operation. Although weak he was mentally clear and his answers were almost too voluble to permit notes. He was completely cooperative, and his whole attitude was exactly like that of other Pers Z.S. people. He was absolutely scientific in his approach and kept fishing for an exchange of information on the subject, appearing surprised at the ignorance of interrogators. In sum, a complete academic, of about B analytic powers.

2. Personal History. Scherschmidt is somewhat over 50 years old. Was a student in 1914, became involved in crypt in the Army, and settled down in Pers. Z. S. soon after the war to make this his life work. Except for the period March 1943 - September 1944, when personal differences caused him to transfer to straight translation work in the document translation section of the A.A., he was with Pers. Z.S. continuously until his capture at ZSCHEPPLIN on 26 April 1945.

3. Crypt Specialties. Scherschmidt was primarily engaged in the linguistic side of cryptanalysis, working on pure codes after the encipherment was removed. (The Polish diplomatic problem was an exception, as the two parts of the problem were inseparable.) Scherschmidt claims to have learned Turkish, Polish and Bulgarian in addition to a smattering of English, French, Russian, and Spanish. He was engaged entirely in Turkish work from 1934 to 1939, and in Polish from 1939 to the end of 1942. While in document translation in 1943-4 he worked on Bulgarian books (and found it very boring), and after his return he did translation and supervision of book-breaking on Turkish codes.

4. Turkish codes. Scherschmidt was not interrogated in detail on his work in Turkish. He said success was very great throughout. In the period 1934-39 the codes were unsystematic (and in Latin at least partially). In 1944-5 the code on which he worked was systematic, with a cyclic additive, and was broken easily.

5. Polish Systems. Scherschmidt worked entirely on diplomatic traffic and was not familiar with military or agent systems or with any successes achieved on them. He had dabbled in Polish throughout his Pers Z.S. career and early in 1939 he was assigned to the main diplomatic code of the Polish Foreign Office. This had been in force since 1934, and some unsuccessful research had been done in an effort to ascertain the encipherment used. The problem was given a very high priority in 1939 and Scherschmidt had first class assistance. With the aid of a captured specimen of encipherment and a captured description of the indicator system, the first message was read early

in 1940. The code was recovered gradually, and in 1941 and 1942 all messages were read, most of them currently. The code went out of use in October 1942 and was replaced by a letter code. Scherschmidt did a little work on this at first but did not come back to the problem later. He said the code was never solved, and he did not know details of the attacks made on it by KUNZE and others.

6. From 1935 to 1942 the Polish Government in Warsaw and later in London used a single unsystematic 4-digit code. The consular services used the diplomatic code of the preceding period. In the diplomatic net a separate pair of encipherment tables was provided for each outstation with one pair for broadcast messages. Scherschmidt remembered traffic to the following points from the Polish Government in LONDON: WASHINGTON (very little), CONSTANTINOPLE, MADRID, MOSCOW, ROME (the VATICAN) and BERN. Scherschmidt could not recall the contents of any of this traffic except that he did recall much talk on the MOSCOW link of negotiations between SIKORSKI and STALIN at one period. Scherschmidt remarked that the German White Paper on Poland included no traffic broken by his section; he was told that its materials were captured.

This is a copy
The original has
been retained under
section 3(4) of the
Public Records Act
1958

PUBLIC RECORD OFFICE

Group/Class HW 40

Piece 181

TICOM/I-63: Page 4 retained under
S3(4) of the PRA 1958

(date) 11/2/2004

(Signed)